ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

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
Admin!	Global Reader
Admin2	Compliance Data Administrator
AdminS	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
Filet.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
User!	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
- 0 years.

Question: 1

DRAG DROP

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.

Actions

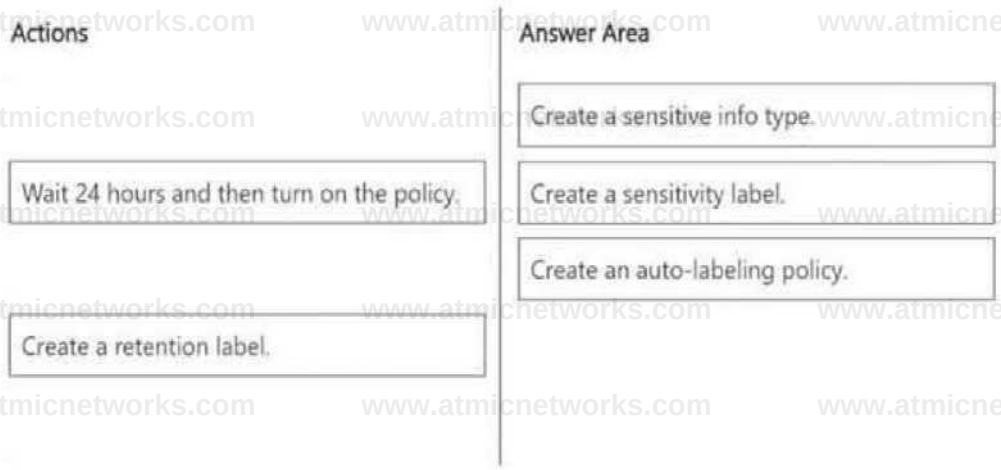
- Create a sensitivity label.
- Wait 24 hours and then turn on the policy.
- Create a sensitive info type.
- Create a retention label.
- Create an auto-labeling policy.

Answer

-
-
-

Answer:

Explanation:



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

Step 1: Create a Sensitive Info Type

- A sensitive info type is needed to detect credit card numbers in documents.
- Microsoft Purview includes built-in sensitive info types for credit card numbers, but we can also create a custom one if necessary.

Step 2: Create a Sensitivity Label

- A sensitivity label is required to classify and protect documents containing sensitive information. • This label can apply encryption, watermarking, or access controls to credit card data.

Step 3: Create an Auto-Labeling Policy

- An auto-labeling policy ensures that the sensitivity label is applied automatically when credit card numbers are detected in Site1.
- This policy is configured to scan files and automatically apply the correct sensitivity label.

Question: 2

You need to meet the technical requirements for the creation of the sensitivity labels.

To which user or users must you assign the Sensitivity Label Administrator role?

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

Answer: D

Explanation:

To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.

Sensitivity Label Administrator Role Responsibilities

This role allows users to:

- Create and manage sensitivity labels in Microsoft Purview.
- Publish and configure auto-labeling policies.
- Modify label encryption and content marking settings.

Review of Admin Roles from the Table:

Admin	Role Assigned	Can Create Sensitivity Labels?
Adminl	Global Reader	□ No read-only permissions.
Admin?	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)
- Adminl (Global Reader) (should be assigned this role to fulfill the requirement that all admins can create labels).

Question: 3

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Create first: ▼

A Compliance Manager assessment
'A content search
A DIP policy
A sensitive info type
A sensitivity label

]

Use for detection method: ▼

Dictionary
File type
Keywords
Regular expression

Answer:

Explanation:

Answer Area

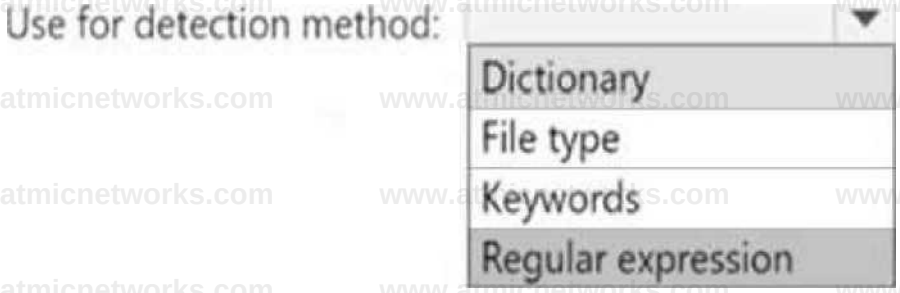
Create first: _____

A Compliance Manager assessment A content search

A DIP policy

A sensitive info type

A sensitivity label



To detect and protect confidential documents, we need a custom rule to identify project codes that start with 999 (since they are classified as confidential).

Box 1: A Sensitive Info Type (SIT) allows Microsoft Purview DLP policies to recognize structured data (e.g., project codes). DLP policies require a sensitive info type to detect content based on patterns,

keywords, or dictionary terms. A sensitivity label alone does not define detection logic—it is used for classification and protection after content is identified.

Box 2: Since project codes follow a structured 10-digit pattern, we should use a Regular Expression (Regex) to match project codes that start with 999.

Example Regex pattern:

999\d{7}

This pattern detects a 10-digit number starting with "999".

Question: 4

HOTSPOT

How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

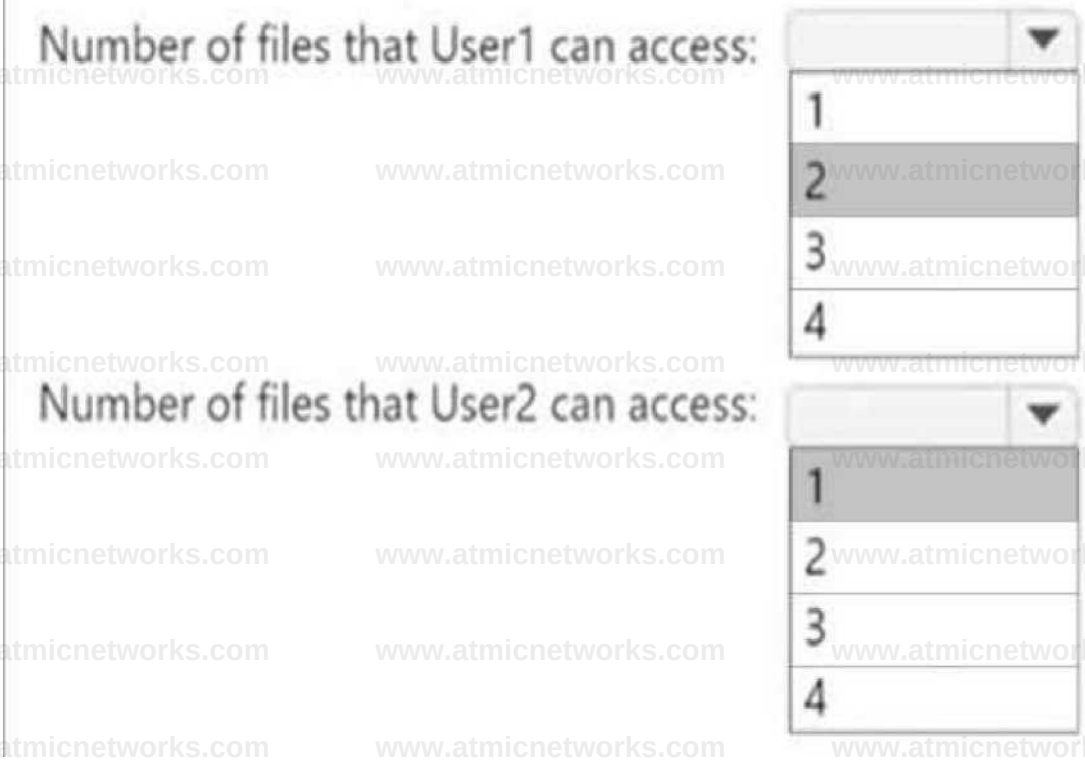
Number of files that Useri can access:

Number of files that User? can access

Answer:

Explanation:

Answer Area



Understanding DLP Policy Impact on File Access

The DLP policy (DLPpolicy1) applies to Site2 and restricts access when: • Content contains SWIFT Codes.

- Instance count is 2 or more.

File Analysis (Based on SWIFT Codes Count)

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
Filel.docx	1	□ No restriction (SWIFT codes < 2)
File2.bmp	4	D Restricted (SWIFT codes > 2)
File3.txt	3	□ Restricted (SWIFT codes > 2)
File4jdsx	7	□ Restricted (SWIFT codes > 2)

Files that remain accessible (not restricted by DLP):

- File1.docx (Contains only 1 SWIFT Code → Below restriction threshold)

User access after DLP policy is applied:

User	Role in Site2	Access Rights	Can Access Files?
Userl	Site Owner	Full Access	Filel.docx, plus override access to another file
User2	Site Visitor	Read-only	Filel.docx only

User1 (Site Owner):

- Has higher privileges and can override DLP restrictions (through admin intervention).
- Can access 2 files (File1.docx + override access to another file).

User2 (Site Visitor):

- Has read-only access but DLP blocks access to restricted files.
- Can only access 1 file (File1.docx), since all others are restricted.

Question: 5

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 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 gOg 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.		

Answer:

Explanation:

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.

Question: 6

You need to meet the retention requirement for the users' Microsoft 365 data.
What is the minimum number of retention policies required to achieve the goal?

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

Answer: B

Explanation:

The requirement states that all Microsoft 365 data for users must be retained for at least one year. In Microsoft 365, retention policies must be configured for each type of data storage.

Step 1: Identifying Where Data is Stored

From the case study, users store data in the following locations:

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

Since these locations fall under two broad categories:

- Microsoft Exchange data (Emails, Public folders)
- SharePoint, OneDrive, and Teams data

Step 2: Required Retention Policies

1 . A single retention policy can cover:

- SharePoint Online
- OneDrive
- Microsoft Teams

2. A second retention policy is required for:

- Exchange (Emails & Public Folders)

Thus, the minimum number of retention policies required to meet the requirement is 2.

Microsoft 365 retention policies can be applied broadly across multiple services with just two policies:

- One for Exchange & Public Folders
- One for SharePoint, OneDrive, and Teams

There's no need for separate policies for each individual workload unless different retention durations are required, which is not stated in the requirement.

Topic 2, Mix Questions

Question: 7

You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1.
Channel1 contains research and development documents.
You plan to implement Microsoft 365 Copilot for the subscription.
You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.
What should you use?

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

Answer: D

Explanation:

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

Question: 8

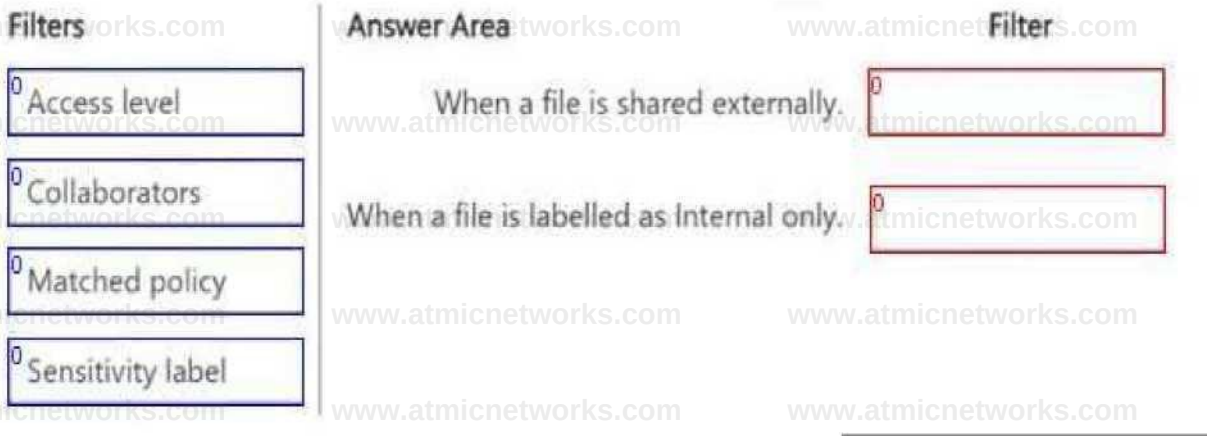
DRAG DROP

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:

Question: 9

HOTSPOT

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
Labell	Any authenticated users: Viewer	Disabled
Label2	*None*	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File!	*None*
File2	Label!
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
Summary!	File!, FileB
Summary2	Fde2
Summary3	Filet 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
Summary 1 has a sensitivity label applied.		EI
Summary2 has a sensitivity label applied.	[9]	[G
Summary3 has a sensitivity label applied.	[O]	[O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Summaryl has a sensitivity label applied.		
Summary? has a sensitivity label applied.		
Summary3 has a sensitivity label applied. O 1 1		

Question: 10

You have a Microsoft 365 E5 subscription.

You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.

Which permission should you select for Label1?

A. Export content(EXPORT)
B. Copy and extract content(EXTRACT)
C. Edit content(DOCEDIT)
D. View rights(VIEW)

Answer: B

Explanation:

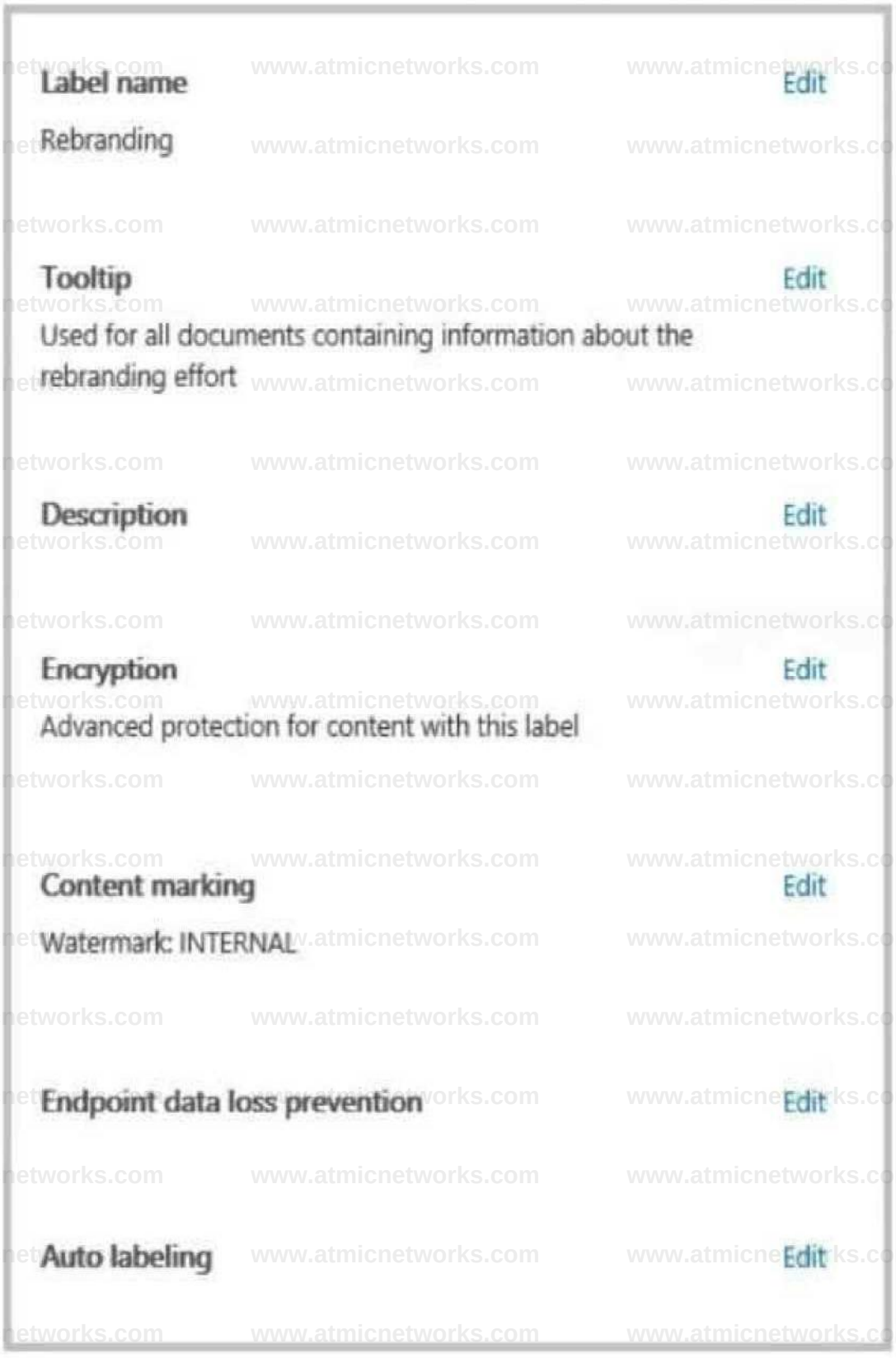
To allow Microsoft 365 Copilot to summarize files that have Label1 applied, the label must grant permission to extract content from the document. The correct permission for this is Copy and extract content (EXTRACT).

Microsoft 365 Copilot requires access to read and process content in documents to generate summaries. The EXTRACT permission allows users (and AI tools like Copilot) to copy and extract content for processing while still maintaining the protection applied by the sensitivity label.

Question: 11

HOTSPOT

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 Area

Statements	Yes	No
All the documents stored on each user s computer will include a watermark automatically. [O]		
If the sensitivity label is applied to a document, the document will have a header that contains the word “INTERNAL".		
The sensitivity label can be applied only to documents that contain the word rebranding. [O]	[O]	[O]

Answer:

Explanation:

Answer Area

Statements	Yes	No
All the documents stored on each user s computer will include a watermark automatically.		
If the sensitivity label is applied to a document, the document will have a header that contains the word “INTERNAL".		
The sensitivity label can be applied only to documents that contain the word rebranding.		

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.

Question: 12

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1.

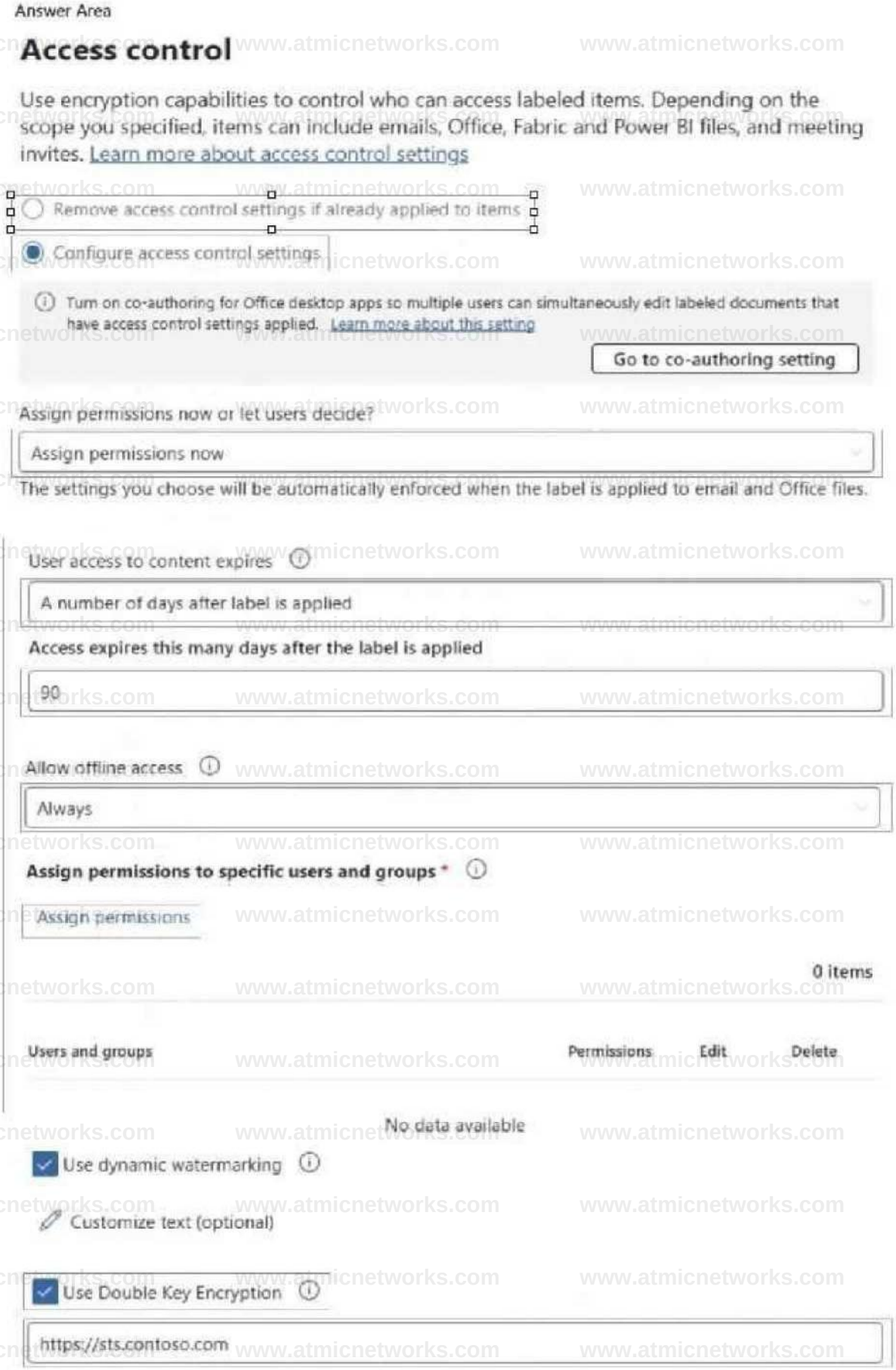
You plan to enable co-authoring for encrypted files.

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:

Explanation:

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

O Remove access control settings if already applied to items

•) Configure access control settings

Q Turn on co-authonng 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 Q

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access Q

Always

Assign permissions to specific users and groups * Q

Assign permissions

0 items

Users and groups Permissions Edit Delete

No data available

Question: 13

HOTSPOT

You have a new Microsoft 365 E5 tenant.

You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area

Action to perform: _____
Create an Exact Data Match (EDM) schema.
Import a data loss prevention (DIP) rule package gStart the opt-in process

To perform the action, assign the role of: Compliance Administrator Global Administrator Security Administrator

Answer:

Explanation:

Answer Area

Action to perform: Create an Exact Data Match (EDM) schema.
Import a data loss prevention (DIP) rule package Start the opt-in process.

To perform the action, assign the role of: Compliance Administrator Global Administrator
Security Administrator

To create a custom trainable classifier in Microsoft Purview (formerly Microsoft Compliance Center), you must first opt into the trainable classifier feature.

Before using custom trainable classifiers, Microsoft requires manual opt-in through the Microsoft Purview compliance portal. Without this step, you cannot create a new classifier.

The Compliance Administrator role has the necessary permissions to configure data classification, DLP policies, and trainable classifiers. Global Administrator has higher privileges but is not required for this task, violating the principle of least privilege. Security Administrator is focused on security- related settings but does not manage compliance features like classifiers.

Question: 14

HOTSPOT

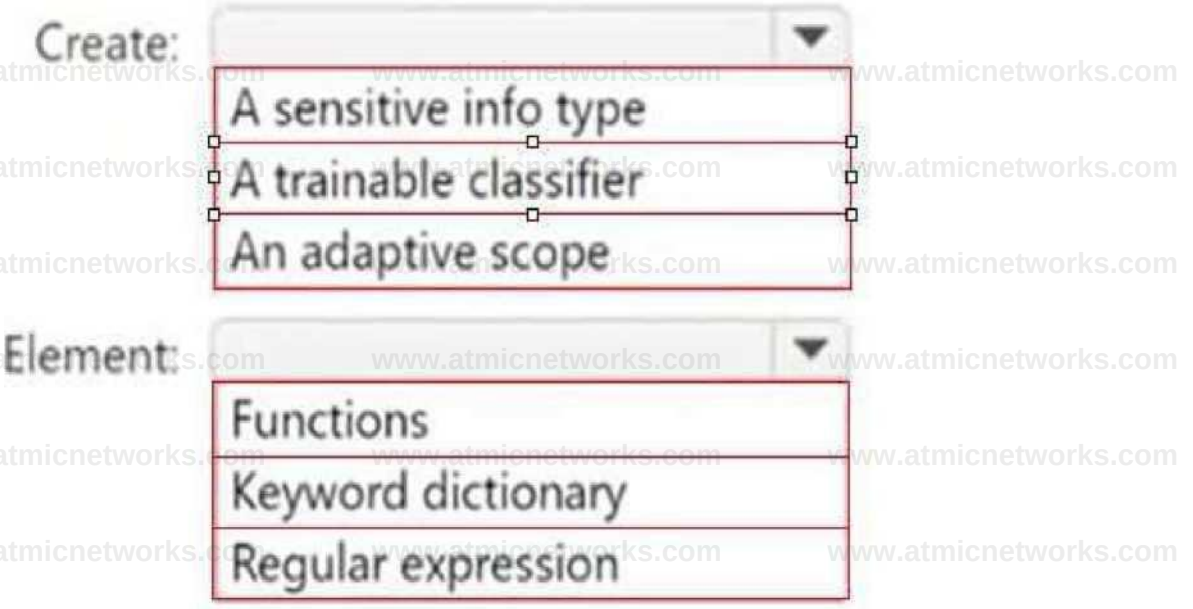
You have a Microsoft 365 E5 subscription.

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

You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint Online library. What should you create in the Microsoft Purview portal, and which type of element should you select? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

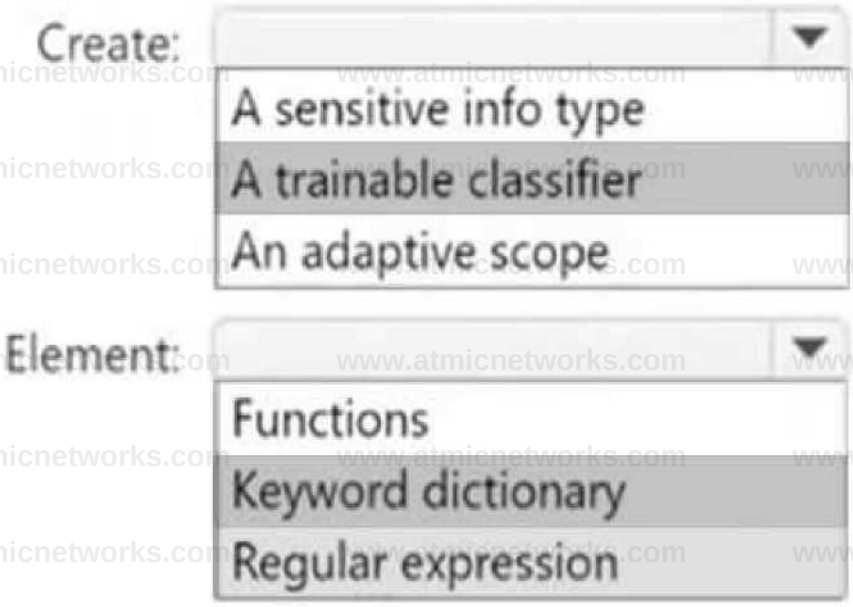
Answer Area



Answer:

Explanation:

Answer Area



Question: 15

You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online.
What should you use?

A. the Microsoft Purview portal
B. the Microsoft Entra admin center
C. the SharePoint admin center
D. the Microsoft 365 admin center

Answer: C

Explanation:

To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center → Settings → Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

Question: 16

You have a Microsoft 365 subscription.

You need to customize encrypted email for the subscription. The solution must meet the following requirements.

- Ensure that when an encrypted email is sent, the email includes the company logo.
- Minimize administrative effort.

Which PowerShell cmdlet should you run?

A. Set-IRMConfiguration
B. Set-OMEConfiguration
C. Set-RMSTemplate
D. New-OMEConfiguration

Answer: B

Explanation:

To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set-OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as:

- Company logo
- Custom text
- Background color

This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

Question: 17

You have a Microsoft 365 E5 subscription.

You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.

What should you configure first?

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

Answer: C

Explanation:

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

- Go to Microsoft Purview compliance portal ^ Information Protection
- Create a sensitivity label
- Enable encryption and configure the content expiration policy
- Publish the label to users

Question: 18

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

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

NOTE: Each correct selection is worth one point.Answer Area

To identify the documents, use a data classification of: ▼

- Exact data match (EDM)
- Sensitive info type
- Trainable classifier

Configure data classifications by using a ▼

- Keyword dictionary
- Regular expression
- Function

Answer:

Explanation:

Answer Area

To identify the documents, use a data classification of: ▼

- Exact data match (EDM)
- Sensitive info type
- Trainable classifier

Configure data classifications by using a. ▼

- Keyword dictionary
- Regular expression
- Function

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 dat

a. 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.

Question: 19

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

You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.

You need to identify and categorize the resumes. The solution must minimize administrative effort. What should you include in the solution?

A. a trainable classifier
B. a keyword dictionary
C. a function
D. an exact data match (EDM) classifier

Answer: A

Explanation:

Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice. Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.

Final Approach:

- Train a trainable classifier using sample resumes.
- Deploy the classifier in Microsoft Purview.
- Configure a sensitivity label to be automatically applied when a document matches the classifier.

Question: 20

HOTSPOT

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

Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label1.

You need to publish Label1 and have the label apply automatically. To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Publish to:

- Site! only
- Group! only
- Group! and Group? only
- Group! and Site! only
- Site! and Team! only
- Group!. Group2, Site!, and Team!

Auto-apply to:

- Site! only
- Group 1 only
- Group! and Group? only
- Group! and Site! only Site! and Team! only
- Group!. Group?, Site!, and Team!

Answer Area

Box 1: Publishing a Sensitivity Label

Sensitivity labels can be published to Microsoft 365 groups, security groups, SharePoint Online sites, and Microsoft Teams. Since we have:

- Groupl (Microsoft 365 group) - Supported
- Group2 (Security group) - Supported
- Site1 (SharePoint Online site) - Supported
- Team1 (Microsoft Teams team) - Supported

This means we can publish Label1 to Group1, Group2, Site1, and Team1.

Box 2: Auto-Applying a Sensitivity Label

Auto-apply policies for sensitivity labels work on:

- SharePoint Online sites (documents)
- OneDrive (documents)
- Exchange email (messages)

However, labels cannot be auto-applied to Microsoft 365 groups or Teams directly because labels are applied to files and emails, not to groups or Teams as entities. Since Site1 (a SharePoint Online site) supports auto-apply, it is the correct option.

Question: 21

HOTSPOT

You have a Microsoft SharePoint Online site that contains the following files.

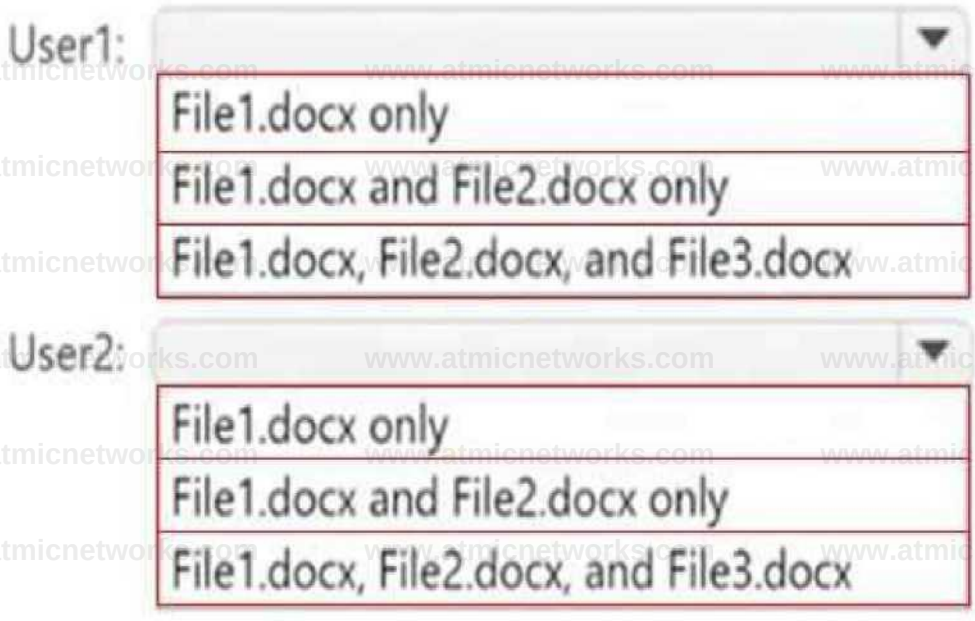
Name	Modified by	Data loss prevention (DLP) action
File! docx	Manageri	*None*
File2.docx	Manageri	Matched by DLP
File3.docx	Manageri	Blocked by DLP

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

Name	Role
Useri	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.

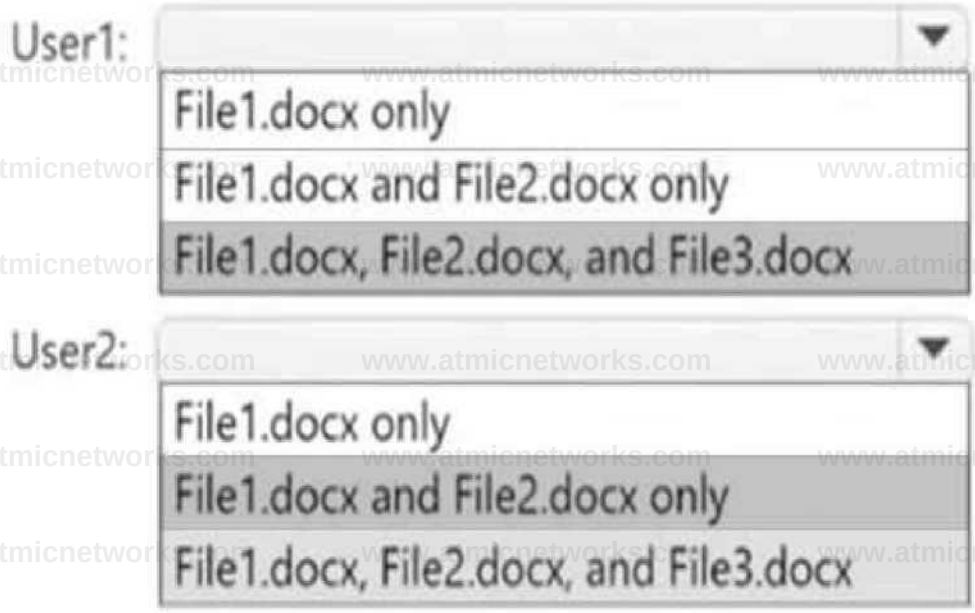
Answer Area



Answer:

Explanation:

Answer Area



Question: 22

You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.

You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:

- If the users are members of a group named Groupl, the users must be allowed to copy the file, and an event must be recorded in the audit log.
- All other users must be blocked from copying the file.

What should you create?

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

Answer: B

Explanation:

To meet the requirements, you need one DLP policy with two separate DLP rules to handle the different conditions:

1. First DLP Rule (For Group1 Members): If the user is a member of Group1 and attempts to copy a file with sensitive data to a USB storage device. Allow the file copy but log the event in the audit log.
2. Second DLP Rule (For All Other Users): If any user who is NOT in Group1 attempts to copy a file with sensitive data to a USB storage device. Block the file transfer.

Question: 23

You have a Microsoft 365 subscription.

You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Microsoft Defender for Cloud Apps, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint ad min center, modify the records management settings.
D. From the Microsoft Purview portal, publish a label.
E. From the Microsoft Purview portal, create a label.

Answer: D, E

Explanation:

To allow users to apply retention labels to individual documents in Microsoft SharePoint libraries, you need to create a retention label and publish the label.

In Microsoft Purview, retention labels define how long content should be retained or deleted. You must first create a label that specifies the retention rules. After creating the label, you must publish it so that it becomes available for users in SharePoint document libraries. Once published, users can manually apply the retention label to individual documents.

Question: 24

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

You need to implement Microsoft Purview data lifecycle management.

What should you create first?

A. a sensitivity label policy
B. a data loss prevention (DLP) policy
C. an auto-labeling policy
D. a retention label

Answer: D

Explanation:

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

Question: 25

You have a Microsoft 365 E5 subscription.

You need to create static retention policies for the following locations:

- Teams chats
- Exchange email
- SharePoint sites
- Microsoft 365 Groups
- Teams channel messages

What is the minimum number of retention policies required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

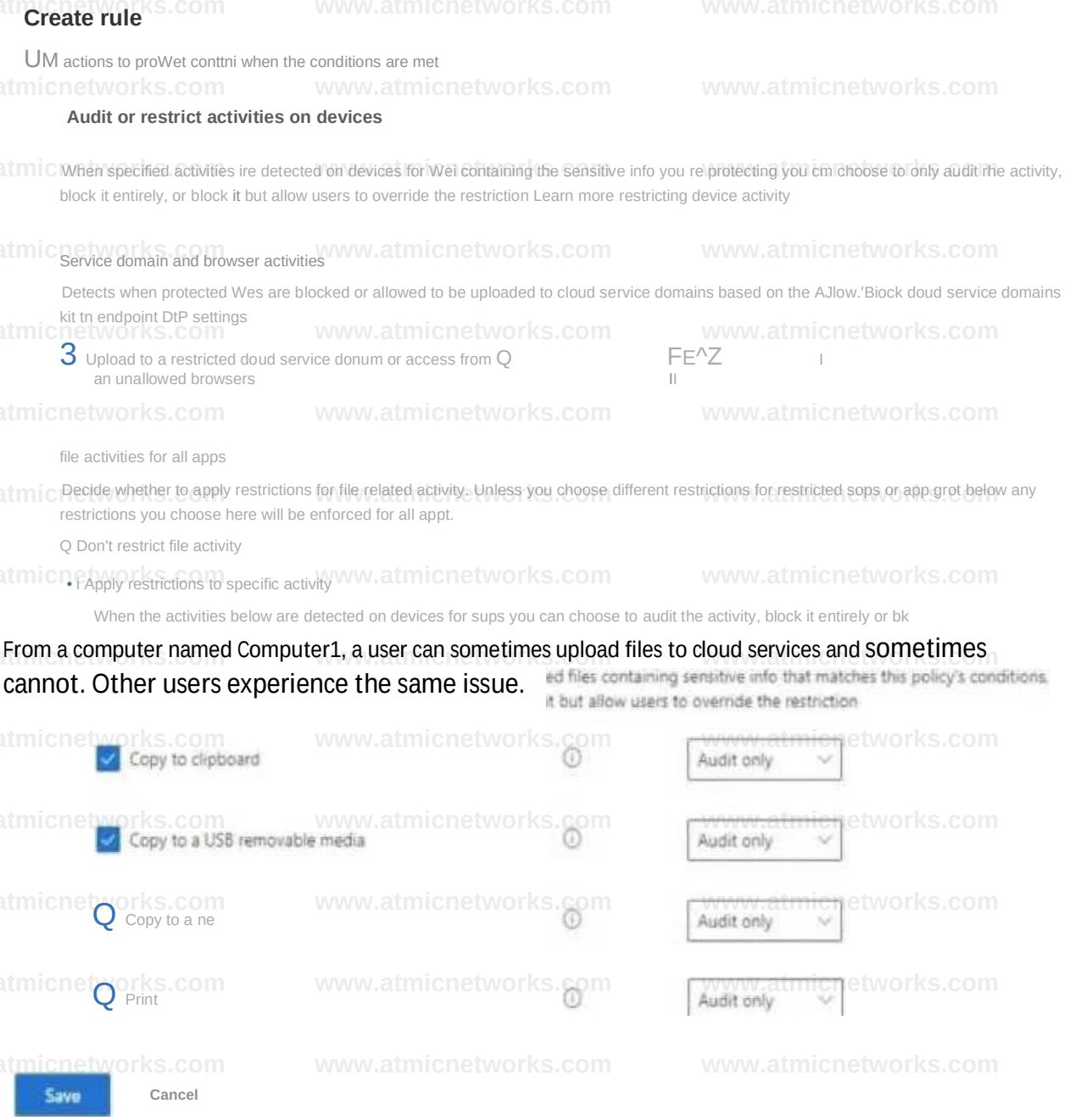
Explanation:

In Microsoft Purview Data Lifecycle Management, different Microsoft 365 locations require separate retention policies because they fall under different storage and compliance models.

Teams Chats & Teams Channel Messages (1 Policy) require a separate retention policy because Teams messages are stored differently than Exchange and SharePoint content. One policy can cover both Teams chats and Teams channel messages. Exchange Email (1 Policy) requires its own separate policy since emails are managed differently than Teams or SharePoint content. SharePoint Sites & Microsoft 365 Groups (1 Policy) are both stored in SharePoint Online, so they can be managed under one policy.

Question: 26

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



From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.

What are two possible causes of the issue? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.

B. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings.

C. The Access by restricted apps action is set to Audit only.

D. The Copy to clipboard action is set to Audit only.

E. The computers are NOT onboarded to Microsoft Purview.

Answer: A, B

Explanation:

The issue where users sometimes can upload files to cloud services and sometimes cannot suggests inconsistent enforcement of Endpoint DLP policies. This can be caused by the unallowed browsers in the Microsoft 365 Endpoint DLP settings are NOT configured. Also, there are file path exclusions in the Microsoft 365 Endpoint DLP settings.

Endpoint DLP can block uploads only when using unallowed browsers. If unallowed browsers are not configured, users might be able to bypass restrictions by switching to a different browser. This could explain why uploads sometimes work and sometimes don't, depending on which browser is used.

File path exclusions allow certain files or folders to be exempt from DLP restrictions. If a specific file location is excluded, files stored there won't trigger DLP policies, leading to inconsistent behavior. This could result in some uploads being blocked while others are allowed.

Question: 27

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	
Location	• Exchange email (All re • SharePoint sites (All si
Retain items for a specific period	5 years (When items were
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1.

You need to modify RP1.

Which two modifications can you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add locations to the policy.
B. Delete the policy.
C. Remove locations from the policy.
D. Decrease the retention period of the policy.
E. Disable the policy.
F. Increase the retention period of the policy.

Answer: A, F

Explanation:

A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.

When a Preservation Lock is applied:

1. You cannot disable or delete the policy.
2. You cannot remove locations from the policy.
3. You cannot decrease the retention period.

4. You can add locations to the policy.
5. You can increase the retention period.

You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

Question: 28

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

Name	Type
Devicel	Windows 11
Device?	Windows 10
DeviceS	iOS
Device4	macOS

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP). Which devices support Endpoint DLP?

A. Device1 only
B. Device1 and Device2 only
C. Device1 and Device4 only
D. Device1, Device2, and Device4 only
E. Device1, Device2, Device3, and Device4

Answer: B

Explanation:

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) is supported only on Windows 10 and Windows 11 devices. It does not support macOS or iOS at this time.
From the provided table:

- Devicel (Windows 11) - Supported
- Device2 (Windows 10) - Supported
- Device3 (iOS) - Not supported
- Device4 (macOS) - Not supported

Thus, only Device1 and Device2 support Endpoint DLP.

Question: 29

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.

Answer Area

AutoApp ly 1:

- 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

Retention 1:

- 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:

Answer Area

AutoApplyl:' 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

Retentionl:'

- 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

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.

Question: 30

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

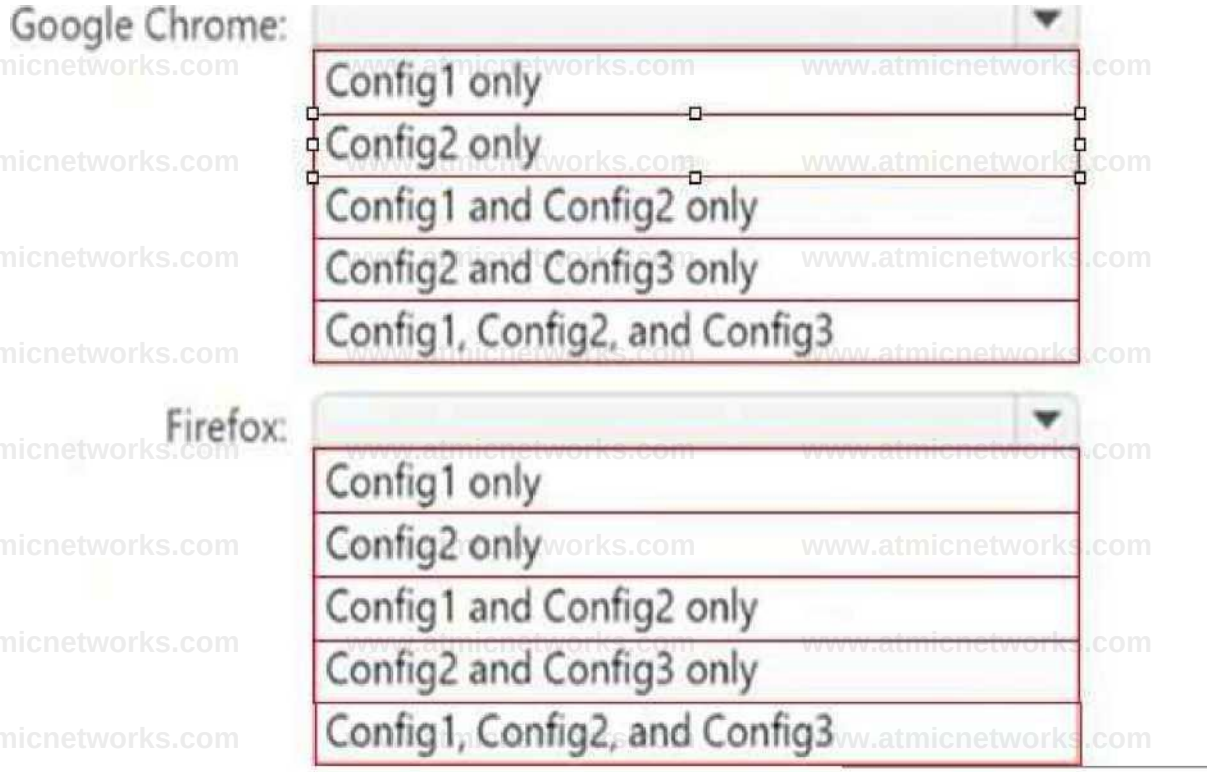
Each configuration uses either Google Chrome or Firefox as a default browser.

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



Answer:

Explanation:

Answer Area

Google Chrome:

- Config 1 only
- Config2 only
- Config 1 and Config2 only
- Config2 and Config3 only
- Config!, Config2, and Config3

Firefox: _____

- Configl only
- Config2 only
- Configl and Config2 only
- Config2 and Config3 only
- Configl, Config2, and Config3

Microsoft Purview browser extensions for Endpoint DLP are supported on:

- Windows 10/11 (Configl)
- 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.

Question: 31

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: B, C

Explanation:

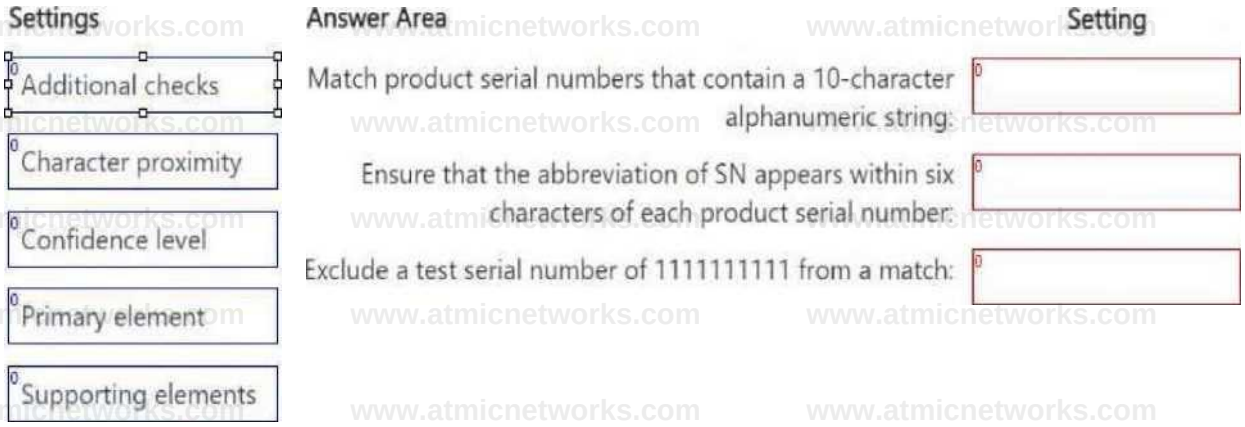
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow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

Question: 32

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:

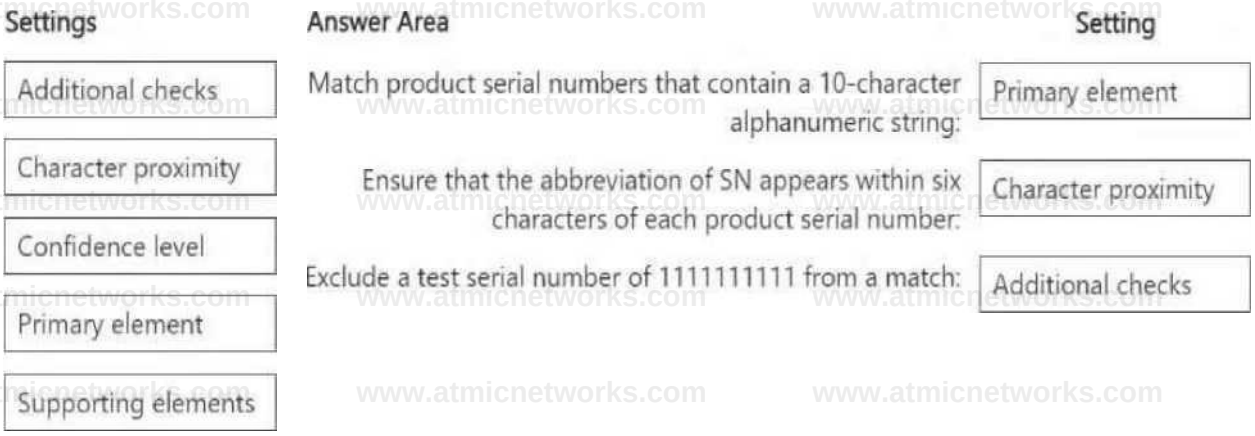
- Match product serial numbers that contain a 10-character alphanumeric string.
- Ensure that the abbreviation of SN appears within six characters of each product serial number.
- Exclude a test serial number of 1111111111 from a match.

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:



Question: 33

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:

- web1.contoso.com
- web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

A. *.contoso.com
B. contoso.com
C. web1.contoso.com and web2.contoso.com
D. web*.contoso.com

Answer: C

Explanation:

The Service domains setting in Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) allows administrators to block or allow specific domains for file uploads. The goal is to prevent users from uploading DLP-protected documents to web1.contoso.com and web2.contoso.com.

Setting the Service domains to "web1.contoso.com and web2.contoso.com" precisely targets the two specific third-party websites, minimizing administrative effort while ensuring strict control.

Question: 34

You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.

You configure an advanced DLP rule in the policy.

Which type of condition can you use in the rule?

A. Sensitive info type
B. Content search query

C. Sensitive label
D. Keywords

Answer: A

Explanation:

When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns. This allows you to apply protection and trigger actions based on the identified content.

Question: 35

HOTSPOT
You plan to create a custom sensitive information type that will use Exact Data Match (EDM).
You need to identify what to upload to Microsoft 365, and which tool to use for the upload. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Upload:

? Data hashes
Data in the XML format
Digitally signed data

Use:

Azure Storage Explorer
EDM upload agent
Microsoft Purview portal
The Set-DlpKeywordDictionary cmdlet

Answer:

Explanation:

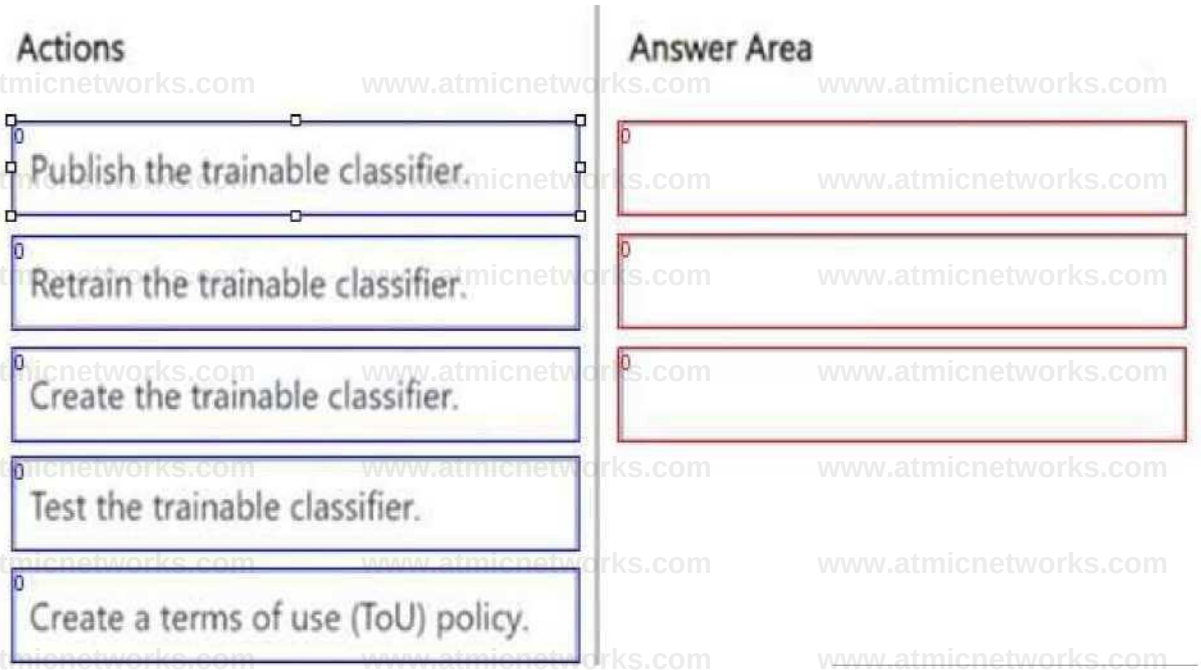
Answer Area

EDM does not store raw data; instead, it requires hashed versions of sensitive data for privacy and security. To upload the hashed data, Microsoft provides the EDM upload agent. This ensures that the data is securely processed and recognized by the EDM service in Microsoft 365.

Question: 36

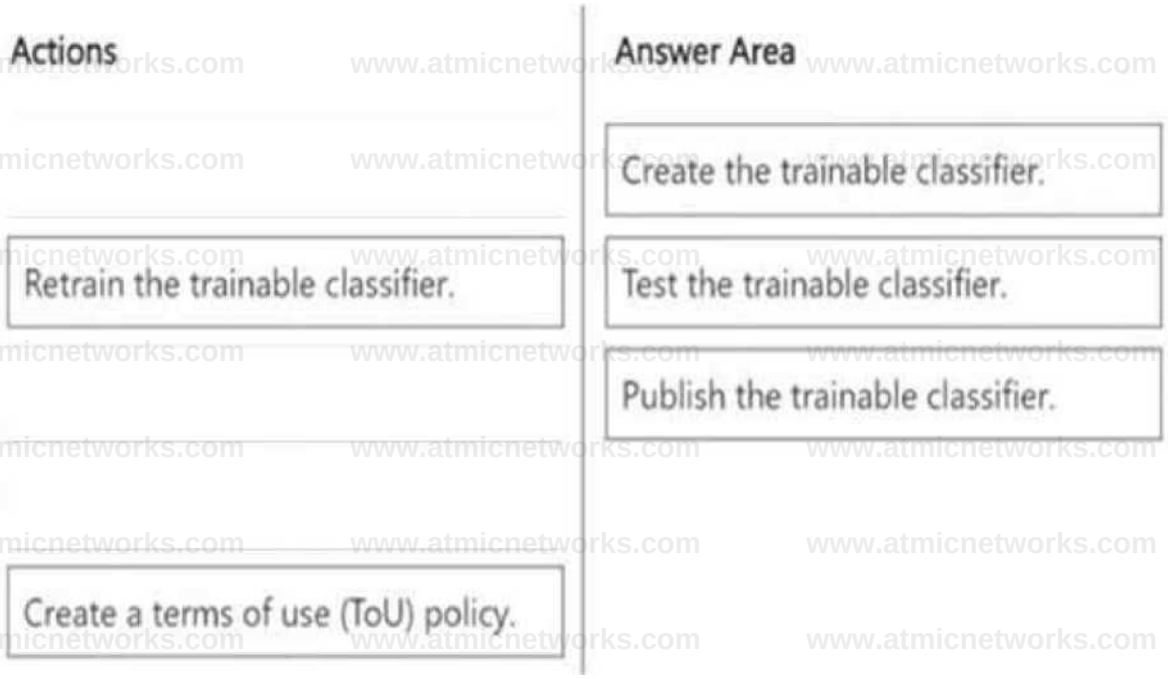
DRAG DROP

You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation:



To create a trainable classifier that can be used in an auto-apply retention label policy, you need to follow these key steps:

1. Create the trainable classifier

This is the first step where you define the classifier, specifying the types of content it should identify.

2. Test the trainable classifier

Before using the classifier in production, you need to validate its accuracy by testing it against sample documents to ensure it correctly classifies the intended data.

3. Publish the trainable classifier

Once testing is successful, you must publish the classifier so that it can be used in policies like autoapply retention labels in Microsoft Purview.

Question: 37

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

A. Connect-IPPSSession
B. Connect-SPOService

C. Connect-ExchangeOnline
D. Connect-MgGraph

Answer: A

Explanation:

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

Question: 38

You receive an email that contains a list of words that will be used for a sensitive information type.
You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list?

A. an XLSX file that contains one word in each cell of the first row
B. an XML file that contains a keyword tag for each word
C. an ACCDB database file that contains a table named Dictionary
D. a text file that has one word on each line

Answer: D

Explanation:

To create a keyword dictionary for a sensitive information type in Microsoft Purview Data Loss Prevention (DLP), you must use a plain text (.txt) file where each keyword is on a separate line.

Format Example (TXT file):
confidential
sensitive
classified
top secret

This format is simple, efficient, and directly compatible with Microsoft 365 DLP policies for keyword dictionaries.

How to use the keyword dictionary?

- Create a text file with one keyword per line.
- Upload it to Microsoft Purview under Data Classification > Sensitive Info Types.
- Use the dictionary in a DLP policy to identify and protect sensitive information.

Question: 39

Your company has a Microsoft 365 tenant.
The company performs annual employee assessments. The assessment results are recorded in a

document named AssessmentTemplate.docx that is created by using a Microsoft Word template. Copies of the

employee assessments are sent to employees and their managers.
The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive folders. A copy of each assessment is also stored in a SharePoint Online folder named Assessments. You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.
What should you include in the solution?

A. Create a fingerprint of AssessmentTemplate.docx.
B. Create a sensitive info type that uses Exact Data Match (EDM).
C. Import 100 sample documents from the Assessments folder to a seed folder.
D. Create a fingerprint of 100 sample documents in the Assessments folder.

Answer: A

Explanation:

Since all employee assessments follow a specific template (AssessmentTemplate.docx), the best way to identify these documents for Data Loss Prevention (DLP) is to create a document fingerprint of that template.
Document fingerprinting allows Microsoft 365 DLP policies to recognize documents based on their structure and format, even when content inside varies (such as different employee names and results). By creating a fingerprint of AssessmentTemplate.docx, any copy derived from that template will be automatically detected by the DLP policy and blocked from being emailed externally.
Steps to implement:

- Create a document fingerprint of AssessmentTemplate.docx using PowerShell and the Microsoft Purview compliance portal.
- Apply a DLP policy to prevent external sharing of documents matching this fingerprint.
- Test the policy by attempting to email an assessment externally.

Question: 40

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.
You are creating an exact data match (EDM) classifier named EDM1.
For EDM1, you upload a schema file that contains the fields shown in the following table.

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

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

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

Answer: B

Explanation:

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

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

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

Question: 41

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
Label 1	Sensitivity label
Label2	Retention label
Pol icy	Retention label policy
DLP1	Data loss prevention (DLP)

Which items can use Trainable 1?

A. Label2 only
B. Label1 and Label2 only
C. Label1 and Policy1 only
D. Label2, Policy1, and DLP1 only
E. Label1, Label2, Policy1, and DLP1

Answer: D

Explanation:

A trainable classifier in Microsoft Purview is used to automatically identify and classify unstructured data based on content patterns. The classifier can be used in:

1. Retention Labels (Label2) ^ Supported

• Trainable classifiers can be linked to retention labels to automatically classify and apply retention policies to documents.

2. Retention Label Policies (Policy1) ^ Supported

• Retention label policies define how and where retention labels are applied, including automatically using trainable classifiers.

3. Data Loss Prevention (DLP) Policies (DLP1) ^ Supported

• Trainable classifiers can be used in DLP policies to detect and protect sensitive content automatically.

Question: 42

You have a Microsoft 365 E5 tenant.
You need to add a new keyword dictionary.
What should you create?

A. a trainable classifier
B. a retention policy
C. a sensitivity label
D. a sensitive info type

Answer: D

Explanation:

To add a new keyword dictionary in Microsoft Purview Data Loss Prevention (DLP), you must create a Sensitive Information Type (SIT).

Sensitive Info Types (SITs) allow you to define custom detection rules, including keyword dictionaries, regular expressions, and functions for identifying sensitive content in emails, documents, and other Microsoft 365 locations. A keyword dictionary is a list of predefined words/phrases that Microsoft Purview can use to identify and classify content for DLP policies.

Steps to add a keyword dictionary:
1. Go to Microsoft Purview compliance portal
2. Navigate to Data classification > Sensitive info types
3. Create a new sensitive info type
4. Add a keyword dictionary
5. Save and use it in a DLP policy

Question: 43

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Adding a folder path to the file path exclusions in Microsoft 365 Endpoint DLP does not prevent Tailspin_scanner.exe from accessing protected sensitive information. Instead, it would exclude those files from DLP protection, which is not the intended outcome.

To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for nonsensitive content.

Question: 44

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

A. Yes
B. No

Answer: B

Explanation:

Creating an app discovery policy in Microsoft Defender for Cloud Apps is used for detecting and monitoring cloud application usage, but it does not prevent a locally installed application (Tailspin_scanner.exe) from accessing sensitive files on Windows 11 devices.

To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for nonsensitive content.

Question: 45

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.

You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.

You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From the Microsoft Defender for Cloud Apps, you mark the application as Unsanctioned. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Marking Tailspin_scanner.exe as "Unsanctioned" in Microsoft Defender for Cloud Apps only blocks its usage in cloud-based activities (such as accessing SharePoint, OneDrive, or Exchange Online).

However, it does not prevent a locally installed application on Windows 11 devices from accessing sensitive files.

To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping

general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for nonsensitive content.

Question: 46

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 a sensitive info type.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.

Mail flow rules (transport rules) can detect sensitive info, but they are limited in encryption capabilities.

DLP policies provide more advanced protection and integration with Microsoft Purview for sensitive info detection.

Question: 47

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted. Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.

A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

Question: 48

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches the text patterns.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.

Text patterns in mail flow rules are not as reliable as sensitive information types in DLP.

Mail flow rules lack advanced content detection and machine learning-based classification, making them less effective than DLP.

Question: 49

HOTSPOT

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DLP) alert shown in the following exhibit.

CO .
oo Contoso Electronics Microsoft Purview

Sensitive info in email with subject 'Message!'

Details Sensitive info types Metadata

Event details

ID

1 ?3fe9«3a65-4lb0-99U-1db451bb*639

Location

Exchange

Time of activity

Jun 6 2022 822 PM

Impacted entities

User

Q Megan Bowen

Email recipients

0 victoriaOfabnkam com

Email subject

Message!

Policy details

DLP policy matched

Policy!

Rule matched

Rule!

Sensitive info types detected

Credit Card Number (19 85%)

Actions taken

GenerateAlert

User overrode policy

Yes

Override justification text

Manager approved

Sensitive info detected in

Document I-docx

Actions | v

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

The email was [answer choice).
- delivered immediately
- quarantined and undelivered sent to a manager for approval

The sender s manager [answer choice).
- approved the email by using a workflow
- overrode Rulel
- was uninvolved in the override process

Answer:

Explanation:

Answer Area

The email was [answer choice) ____ ____ X
- delivered immediately
- quarantined and undelivered sent to a manager for approval

The sender s manager [answer choice].
- approved the email by using a workflow
- overrode Rulel
- was uninvolved in the override process

Question: 50

HOTSPOT

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

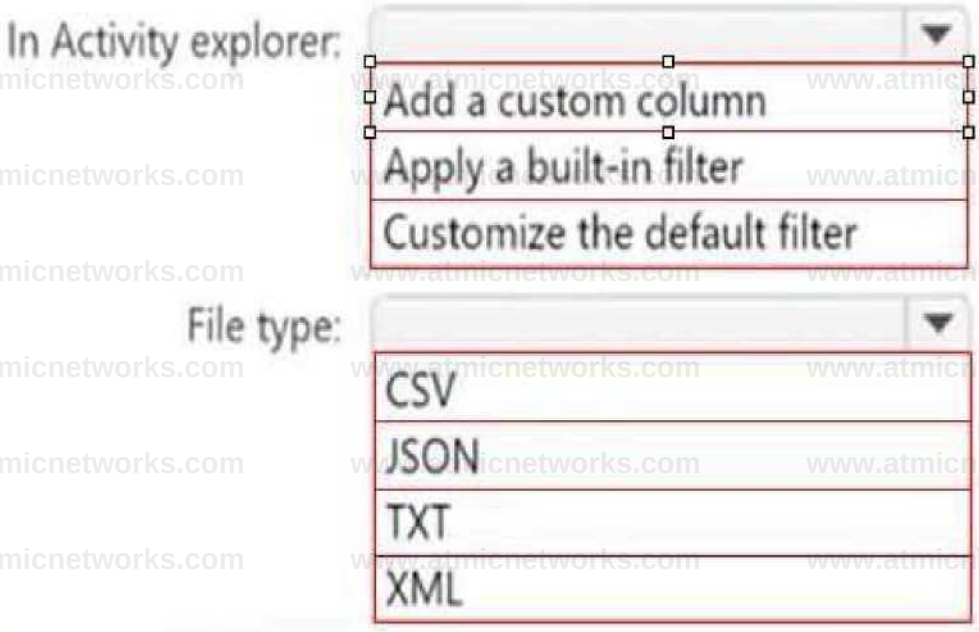
You plan to export DLP activity by using Activity explorer.

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

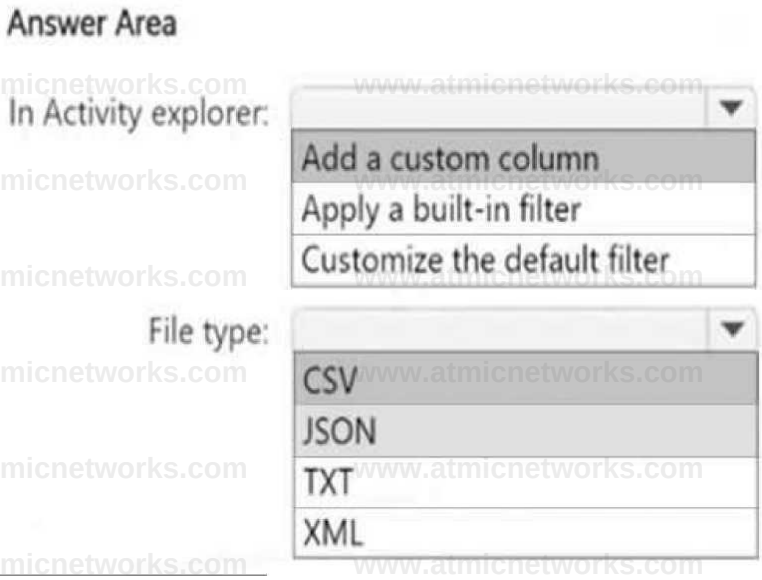


Answer:

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.



Question: 51

DRAG DROP

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies.

You need to identify the following:

- Rules that are applied without triggering a policy alert
- The top 10 files that have matched DLP policies
- Alerts that are miscategorized

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

NOTE: Each correct selection is worth one point.

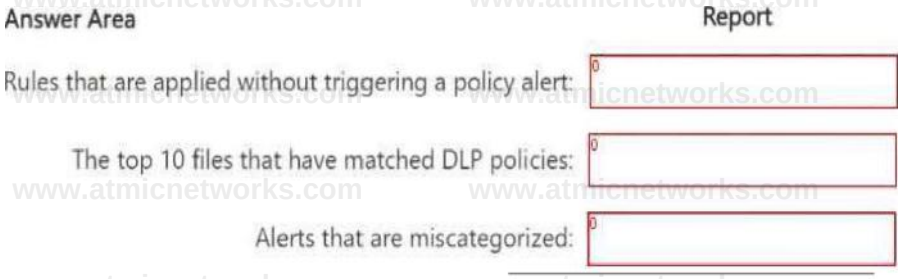
Reports

9 DLP policy matches

False positive and override

Incident reports

The False positive and override report helps identify rules that were applied but did not generate an actual policy alert, which means they were overridden or deemed false positives.



Answer:

Explanation:

Reports

DLP policy matches

False positive and override

Incident reports

The DLP policy matches report provides details on files that matched DLP policies, including the top 10 files.

The Incident reports report helps analyze and review alerts, including those that may have been miscategorized.

Question: 52

HOTSPOT

You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

The subscription contains the users shown in the following table.

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

You need to review the activities.

What should you use for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Useri; *

Activity explorer in Data Security Posture Management for AI (DSPM for AI)

°Audit loo search 5

□ □ □

Insider risk audit log

Unified Catalog

User?: _____ *

Activity explorer in Data Security Posture Management for AI (DSPM for AI) Audit log search

Insider risk audit log

Unified Catalog

User3 ,

Activity explorer in Data Security Posture Management for AI (DSPM for AI) Audit log search

Insider risk audit log

Unified Catalog

_____

Answer:

Explanation:

Answer Area

Useri:

Activity explorer in Data Security Posture Management for AI (DSPM for AI) Audit log search

Insider risk audit log _____

Unified Catalog

User2: _____

Activity explorer in Data Security Posture Management for AI (DSPM for AI) Audit log search

Insider risk audit log

Unified Catalog

User3

Activity explorer in Data Security Posture Management for AI (DSPM for AI) Audit log search

Insider risk audit log

Unified Catalog

User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.

User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI-related activity cannot be tracked in DSPM for AI. Instead, Audit log search should be used to review activity such as using Microsoft 365 Copilot.

User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

Question: 53

HOTSPOT

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

You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duratu
10	AuditRetentionl	Exchangeitem	MailboxLogin	*None*	90
20	AuditRetention2	Exchanqeltem	MailltemsAccesssed	. User!	9 Month
30	AuditRetention3	Sharepoint	*None*	Userl	6 Month
40	AuditRetention4	Sharepoint	SiteRenamed	Userl	9 Month
50	AuditRetentionS	Sharepoint	SiteRenamed	*None*	10

The users perform the following actions:

- Userl renames a Microsoft SharePoint Online site.
- User2 sends an email message.

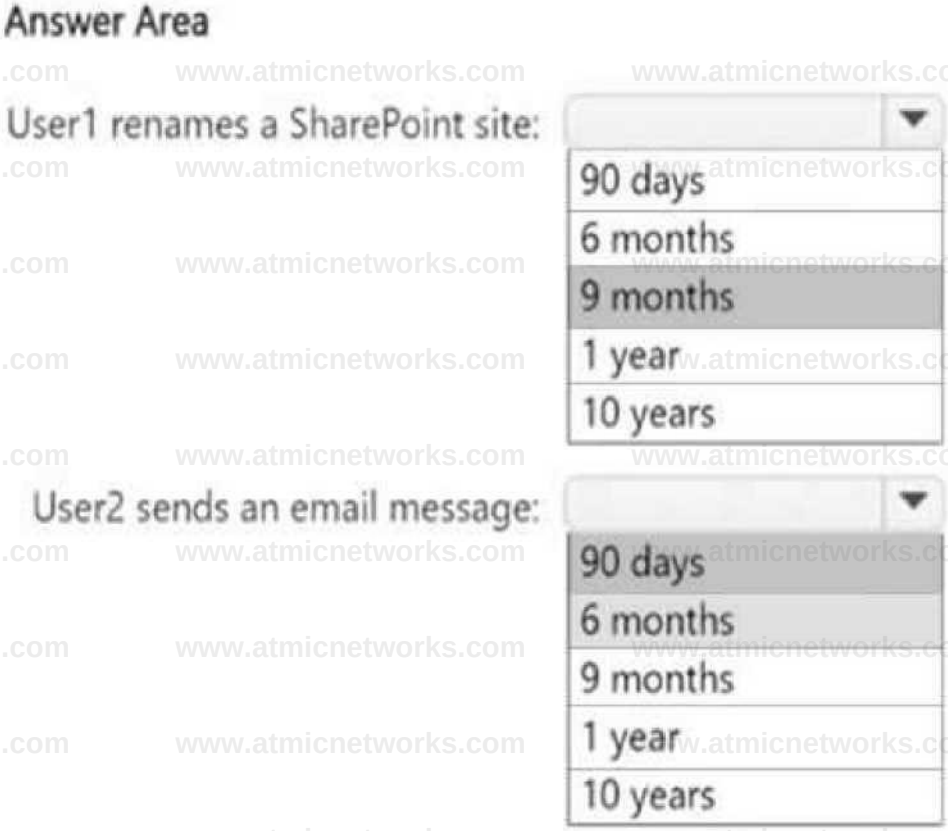
How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:



The action "SiteRenamed" for SharePoint is covered under the AuditRetention4 policy, which applies to User1 and retains logs for 9 months.

The action "Send" for ExchangeItem is covered under the AuditRetention2 policy, but this policy applies only to User1. Since User2 is not covered under a specific policy, the default retention period for audit logs in Microsoft Purview is 90 days.

Question: 54

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

Name	Description
Useri	• User 1 is a regional manager. • Useri is assigned the Reader role • Three department managers report to Useri.
User2	• User2 is the human resources (HR) department manager. • User2 has no Microsoft Entra roles assigned. • Five HR department users report to User2.
User3	• User3 is a developer. • User3 reports to User2. • User3 is the only user in the compliance department. • User3 is assigned the Compliance Administrator role.
User4	• User4 is the assistant of Useri. • User4 has no Microsoft Entra roles assigned. • User4 handles a high volume of confidential data on behalf of User!

Which users will Microsoft Purview insider risk management flag as potential high-impact users?

A. User1 and User2 only
B. User2 and User3 only
C. User1, User2, and User3 only
D. User1, User2, User3, and User4

Answer: D

Explanation:

Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:

User1 (Regional Manager, assigned Reader role, manages department managers)

Risk Factors:

- Holds a managerial position (regional manager).
- Manages multiple department managers, indicating organizational influence.
- Access to critical business information.

Flagged? -Yes (Managerial role and access to confidential data).

User2 (HR department manager, no Microsoft Entra roles, manages HR department users)

Risk Factors:

- Manages HR department users, meaning they likely handle sensitive employee data.
- HR roles are often considered high-risk due to access to personal and payroll data.

Flagged? -Yes (HR role and access to sensitive employee data).

User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role)

Risk Factors:

- Compliance Administrator role grants access to sensitive security and regulatory data.
- Only person in the compliance department, meaning they hold a critical role.
- Potentially high impact on compliance and security settings.

Flagged? -Yes (Privileged Compliance Administrator role).

User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1)

Risk Factors:

- Handles a high volume of confidential data on behalf of a regional manager.
- Assistants with access to sensitive data are considered insider risk candidates.

Flagged? -Yes (High access to sensitive information).

Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

Question: 55

You have a Microsoft 365 E5 subscription.
You need to review a Microsoft 365 Copilot usage report.
From where should you review the report?

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

Answer: C

Explanation:

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

interactions within Microsoft 365.

Question: 56

You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview insider risk management.
You implement the HR data connector.
You need to prepare the data that will be imported by the data connector.
In which format should you prepare the data?

A. JSON
B. CSV
C. TSV
D. XML
E. PRN

Answer: B

Explanation:

When implementing Microsoft Purview Insider Risk Management and using the HR data connector, you must prepare HR data in CSV (Comma-Separated Values) format. This format is required because Microsoft Purview supports CSV files for importing user employment details, termination dates, role changes, and other HR-related attributes.

Question: 57

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

Explanation:

To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative effort, you should first create a security group in Microsoft Entra ID (formerly Azure AD).

Security groups allow you to scope insider risk management policies to specific users instead of applying policies to all users, which helps in minimizing unnecessary alerts and reducing administrative overhead. After creating the security group, you can assign this group to a Microsoft Purview Insider Risk Management policy, ensuring that only project-related users are affected.

Question: 58

You have a Microsoft 365 E5 subscription. The subscription contains 500 devices that are onboarded to Microsoft Purview.
You select Activate Microsoft Purview Audit.
You need to ensure that you can track interactions between users and generative AI websites.
What should you deploy to the devices?

A. the Microsoft Purview extension
B. the Microsoft Purview Information Protection client
C. the Microsoft Defender Browser Protection extension
D. Endpoint analytics

Answer: A

Explanation:

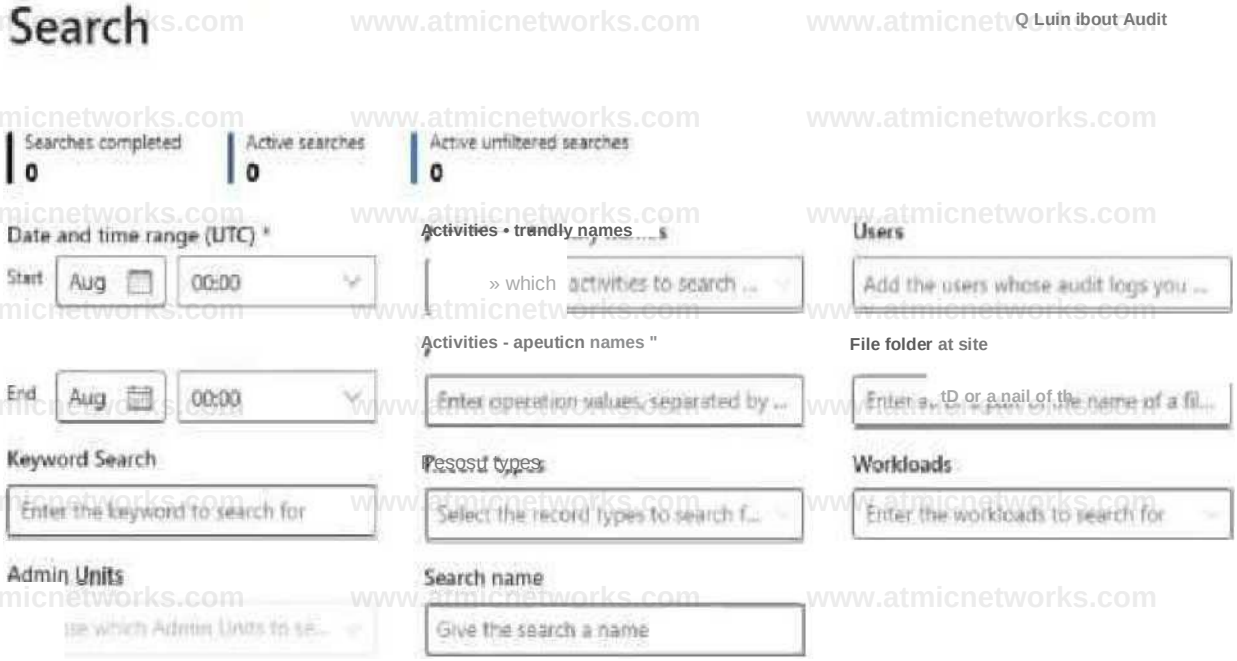
To track interactions between users and generative AI websites in Microsoft Purview Audit, you need to deploy the Microsoft Purview browser extension to the devices. This extension enables tracking of user activities on web-based applications, including AI-related tools like ChatGPT, Microsoft Copilot, and other generative AI platforms.

Microsoft Purview extension provides visibility into browser-based activities, including AI tool usage, ensuring compliance and risk management within Microsoft Purview. This extension works with Microsoft Edge and Google Chrome to track and log user interactions.

Question: 59

HOTSPOT
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.

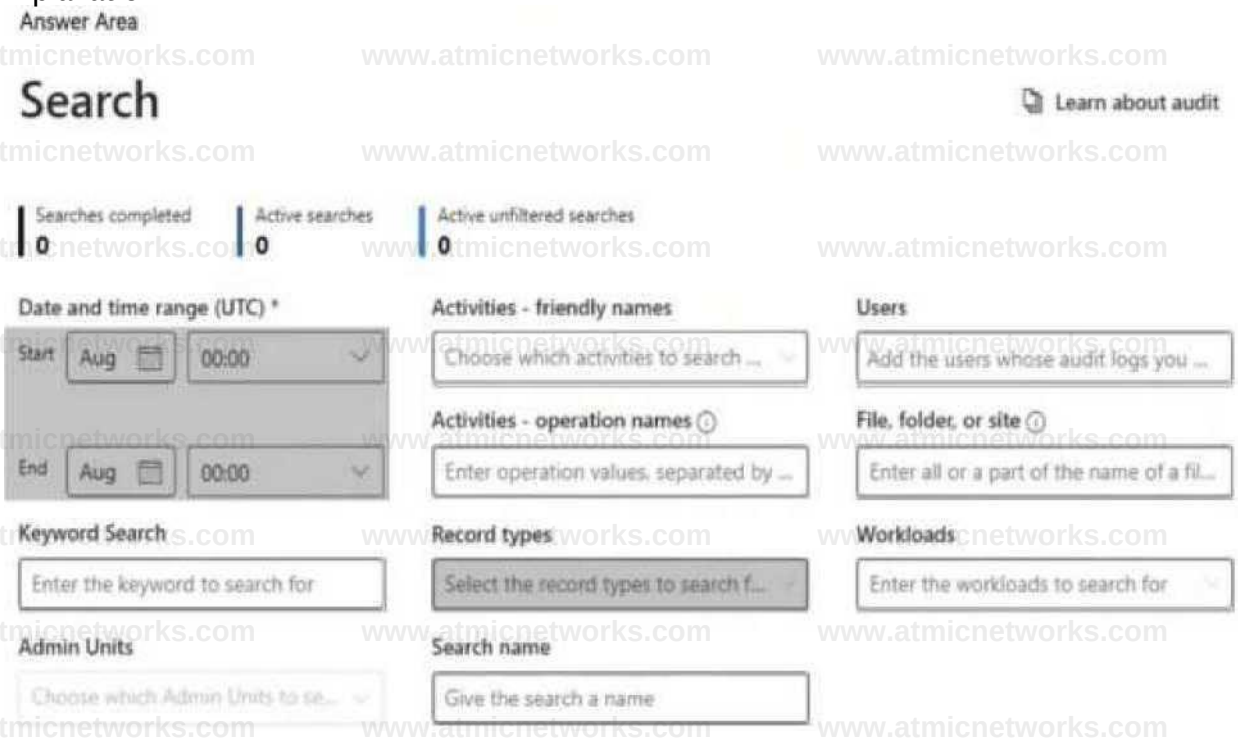
Answer Area



Answer

Explanation:

Answer Area



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.

Question: 60

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

You create a communication compliance policy named Policy1 and select Detect Microsoft Copilot interactions.

Which two trainable classifiers will be added to Policy1 automatically? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: A, E

Explanation:

When you create a communication compliance policy in Microsoft Purview and select "Detect Microsoft Copilot interactions," certain trainable classifiers are automatically added to help detect sensitive or inappropriate AI usage.

The "Unauthorized disclosure" classifier helps detect cases where users might share confidential or sensitive information via Copilot interactions, preventing unintended data leaks. The "Protected Materials" classifier is used to identify sensitive or restricted content that should not be shared through Copilot, ensuring compliance with organizational policies.

Question: 61

Your company has offices in multiple countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management.

You plan to perform the following actions:

- In a new country, open an office named Office1.
- Create a new user named User1.
- Deploy insider risk management to Office1.
- Add User1 to the Insider Risk Management Admins role group.

You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.

What should you create first?

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

Answer: C

Explanation:

To ensure User1 can perform insider risk management tasks only for the users and devices in Office1, the first step is to create an administrative unit in Microsoft Entra ID (formerly Azure AD).

Administrative units allow you to scope permissions to specific users, devices, and locations. By creating an administrative unit for Office1 and assigning User1 to the Insider Risk Management Admins role group within that unit, User1 will only have access to users and devices in Office1.

Question: 62

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

- Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.
- Integrates data loss prevention (DLP) capabilities with insider risk management.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Captures clips of key security-related user activities. ,

Adaptive scopes

□Classifiers □

□ □ □

Forensic evidence

Search

Integrates DLP capabilities with insider risk management *

Adaptive Protection

eDiscovery (Premium)

Records management

Trainable classifiers

Answer:

Explanation:

Answer Area

Captures clips of key security-related user activities: I

Adaptive scopes

Classifiers Forensic evidence I

Search

Integrates DIP capabilities with insider risk management:

Adaptive Protection

eDiscovery (Premium)

Records management

Question: 63

You have a Microsoft 365 subscription.

Users have devices that run Windows 11.

You plan to create a Microsoft Purview insider risk management policy that will detect when a user performs the following actions:

- Deletes files that contain a sensitive information type (SIT) from their device
- Copies files that contain a SIT to a USB drive
- Prints files that contain a SIT

You need to prepare the environment to support the policy.

What should you do?

A. Configure the physical badging connector.
B. Configure the HR data connector.
C. Create a Microsoft Purview communication compliance policy.
D. Onboard the devices to Microsoft Purview.

Answer: D

Explanation:

To ensure that Microsoft Purview Insider Risk Management can detect file deletions, USB copies, and print actions on sensitive information, you must onboard the Windows 11 devices to Microsoft Purview.

Device onboarding enables endpoint activity monitoring, allowing Purview to track and log user activities such as file deletions, USB transfers, and printing of sensitive files. Once onboarded, the Insider Risk Management policy can analyze these activities and generate risk alerts when sensitive information types (SITs) are involved.

Question: 64

HOTSPOT

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 Area

Explanation:

Answer Area

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.

Question: 65

HOTSPOT

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

You need ensure that an incident will be generated when a user visits a phishing website.

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

NOTE: Each correct selection is worth one point.

Answer Area

Type of policy to create: ▼ a Communication compliance
T ---------- ° ---------- T
4 a Data loss prevention (DIP) p ------ D r an Insider risk management

Prerequisite to complete:
Create a sensitive service domain group.
Deploy the Microsoft Defender Browser Protection extension. Deploy the Microsoft Purview extension.
From Data Loss Prevention, configure the Service domains settings

Answer:

Explanation:

Answer Area

Type of policy to create: T
a Communication compliance a Data loss prevention (DIP) an Insider risk management

Prerequisite to complete:
Create a sensitive service domain group.
Deploy the Microsoft Defender Browser Protection extension. Deploy the Microsoft Purview extension.
From Data Loss Prevention, configure the Service domains settings.

Box 1: Insider Risk Management policies in Microsoft Purview can be configured to detect risky behavior, such as accessing phishing websites. These policies monitor user activity, generate alerts,

and help organizations investigate potential security threats.

Box 2: Microsoft Defender Browser Protection extension helps in detecting unsafe or phishing websites and integrating this detection with Insider Risk Management policies. This extension works with Microsoft Edge and

Google Chrome to identify risky browsing activity and trigger alerts.

Question: 66

You have Microsoft 365 E5 subscription.

You create two alert policies named Policy1 and Policy2 that will be triggered at the times shown in the following table.

Policy	Time (hh:mm:ss)
Policyl	10:00:00
Policy?	10:00:03
Policyl	10:00:04
Policy?	10:00:31
Policyl	10:01:01
Policyl	10:04:45

How many alerts will be added to the Microsoft Purview portal?

A. 2
B. 3
C. 4
D. 5
E. 6

Answer: D

Explanation:

In Microsoft Purview, when multiple alert policies trigger alerts, duplicate alerts within a short period (typically 5 minutes) may be suppressed to avoid redundancy.

Step-by-step Analysis:

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policyl	10:00:00	Yes
Policy2	10:00:03	Yes
Policyl	10:00:04	No (Duplicate within 5 min)
Pol icy 2	10:00:31	No (Duplicate within 5 min)
Policyl	10:01:01	Yes
Policyl	10:04:45	Yes

- Policyl at 10:00:04 is ignored because Policyl already triggered at 10:00:00, and it's within 5 minutes.
- Policy2 at 10:00:31 is ignored because Policy2 already triggered at 10:00:03, and it's within 5 minutes.
- Policy1 at 10:01:01 is a new alert because it's over 1 minute after the previous Policy1 alert.
- Policy1 at 10:04:45 is a new alert because it's over 3 minutes after the previous Policy1 alert.

Question: 67

HOTSPOT

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

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

You plan to create a Microsoft Purview insider risk management case named Case1.

Which insider risk management object should you select first, and which users will be added as contributors for Case1 by default?

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

NOTE: Each correct selection is worth one point.

Answer Area

Object: *

- An alert
- A policy
- A risky user
- A notice template
- Forensic evidence

Users I _____ v

Admin! and Admin? only

Admin? and AdminS only

AdminS and Admin4 only

AdminZ, AdtninS, and Admin4 only

Admm1. Admin?, Admin3, and AdminA

Answer:

Explanation:

Answer Area

Object: v

An alert

A policy

A risky user

A notice template

Forensic evidence

Users: | _____

Admin! and Admin2 only

Admin2 and Admin3 only

Admin3 and Admin4 only

Admin2, Admin3, and Admin4 only

Admin!, Admin2, Admm3. and Admin4

Box 1: When creating a Microsoft Purview Insider Risk Management case, you must first select a risky user to investigate. The case will be built around this specific user's activities, linking alerts and risk

signals to the investigation.

Box 2: The Insider Risk Management role groups determine who can access and contribute to cases:

- Adminl (Insider Risk Management Admins) ^ Full admin access.
- Admin2 (Insider Risk Management Analysts) ^ Analysts who review cases.
- Admin3 (Risk Management Investigators) ^ Investigators who work on cases.
- Admin4 (Insider Risk Management Auditors) ^ Auditors who oversee cases.

All these roles have default access to insider risk cases in Microsoft Purview, so all four admins are added as contributors.

Question: 68

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. The subscription contains the users shown in the following table.

Name	JIT protection scope
Useri	Included
User2	Not configured
User3	Included

The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device 1	Onboarded
Device?	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

Name	File classification evaluation status	Location
Filel.docx	Not evaluated	Device 1
File2.pdf	Evaluated	Device?
FileS.xlsx	Not evaluated	Device3

No.

For each of the following statements, select Yes if the statement is true. Otherwise, select NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Explanation:

Answer Area

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

Statement 1 - No. User1 is included in JIT protection. File1.docx is on Device1, which is onboarded to Microsoft Defender. However, File1.docx has not been evaluated for file classification, meaning JIT cannot enforce protection on it. If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.

Statement 2 - No. User2 is not configured for JIT protection (JIT does not apply to them). File2.pdf has been evaluated for classification, but since User2 is not included in JIT protection, no blocking occurs. If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.

Statement 3 - No. User3 is included in JIT protection. However, Device3 is not onboarded to Microsoft Defender, meaning JIT protection cannot enforce actions on it. File3.xlsx has not been evaluated, so even if the device were onboarded, JIT would not have classification data to act upon.

Question: 69

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.
What should you do?

A. From the Microsoft Purview portal create an insider risk policy
B. From the Microsoft Defender portal create a file policy
C. From the Microsoft Defender portal, create an activity policy.
D. From the Microsoft Purview portal, start a data investigation.

Answer: B

Explanation:

An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.

Question: 70

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

Explanation:

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.

Question: 71

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
Solution: You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled $true - AdminAuditLogCmdlets *Mailbox* command.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

The Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox* command is

incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

Question: 72

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

Solution: You run the Set-Mailbox -Identity "User1" -AuditEnabled $true command.

Does that meet the goal?

A. Yes

B. No

Answer: A

Explanation:

To track who accesses User1's mailbox, you need to enable mailbox auditing for User1. By default, Exchange mailbox auditing is not enabled per mailbox (even though it is enabled tenant-wide).

The Set-Mailbox -Identity "User1" -AuditEnabled $true command enables audit logging for mailbox actions like:

- Read emails
- Delete emails
- Send emails as User1
- Access by delegated users

Once enabled, you can search for future sign-ins and actions in the Microsoft Purview audit logs.

Question: 73

You have a data loss prevention (DIP) policy that applies to the Devices location. The policy protects documents that contain United States passport numbers

Users report that they cannot upload documents to a travel management website because of the pokey.

Vou need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.

Which Microsoft 365 Endpoint data loss prevention (Endpoint DIP) setting should you configure?

A. Service domains
B. Unallowed browsers
C. File path exclusions
D. Unallowed apps

Answer: A

Explanation:

Question: 74

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site! and the data loss prevention (DLP) policies shown in the following table.

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown In the following table.

Rule	User notifications	Policy «P	If there's a match for this rule, stop processing additional DIP policies and rules
Rulel	On	Tip 1	Enabled
Ruit2	On	Tip 2	Disabled
Rule?	On	Tip 3	Enabled
Ruled	On	Tip 4	Disabled

All the policies are assigned to Site1.

You need to ensure that if a user uploads a document to Site1 that matches all the rules, the user will be shown the Tip 2 policy tip. What should you do?

A. Change the priority of DLP2 to 0.
B. Prevent additional processing of the policies if there is a match for Rule2
C. Change the priority of DLP2 to 3.
D. Enable additional processing of the policies if there is a match for Rule1.

Answer: B

Explanation:

Question: 75

HOTSPOT

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

Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
Rule4	3	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off

You need to identity which rules will apply when content matches multiple advanced DIP rules.

Which rules should you identify? To answer, select the appropriate options in the answer area.

Answer:

Explanation:

Answer Atm

1 content matches Rule' Rule?, and Rule] Only Rule! tikes effect

lent matches Rule?, Rule], and Rukut Rule? Rule] and Rule4 take effect

Question: 76

HOTSPOT

You have a Microsoft 36S subscription that contains the users shown in the following table.

Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

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

Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	None	Send an incident report to the administrator.	None

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

Answer Area

Statements	Yes	No
If Uteri sends an email message that contains tree credit card numbers to user4@fabnkam com. the message will be encrypted		
If Uteri sends an email message that contains five credit card numbers to orders@adatum.com the message will be encrypted and delivered.		
If User? sends an email message that contains five credit card numbers to orders@adatirm corn the message will be encrypted and delivered		

Answer:

Explanation:

Answer Area

Statements
If Useri sends an email message **that** contains five credit card numbers to user4@fabnkam.com. the message will be encrypted
If Uteri tends an email message that contains five credit card numbers to orders@adaturn com the message will be encrypted and delivered
If User? sends an email message that contains five credit card numbers to orders@adatum.com the message will be encrypted and defaveted.

&

Question: 77

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

Explanation:

Question: 78

HOTSPOT
You have a Microsoft 36S ES subscription

You need to implement Endpoint data loss prevention (Endpoint DLP) to meet the following requirements:

- Ensure that users can upload data to only two sites named Site1 and Site2.
- Prevent users from pasting data to two search engines named Search1 and Search2.
- Minimize the number of policies and groups.

What If the minimum number of sensitive service domain groups and Endpoint DIP policies required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sensitive service domain groups [*]

1

ipoint DIP policies

4

Answer:

Explanation:

Answer Area

Sensitive service domain groups

Endpoint DIP policies

Question: 79

You have a Microsoft 565 E5 tenant that uses Microsoft Teams and contains two users named User1 and User2.

You create a data Joss prevention (DIP) policy that is applied to the Teams chat and channel messages location for User1 and User?

Which Teams entities will have DLP protection?

A. 1:1/n chats and general channels only
B. 1:1/n chats and private channels only
C. 1:1/n chats, general channels, and private channels

Answer: C

Explanation:

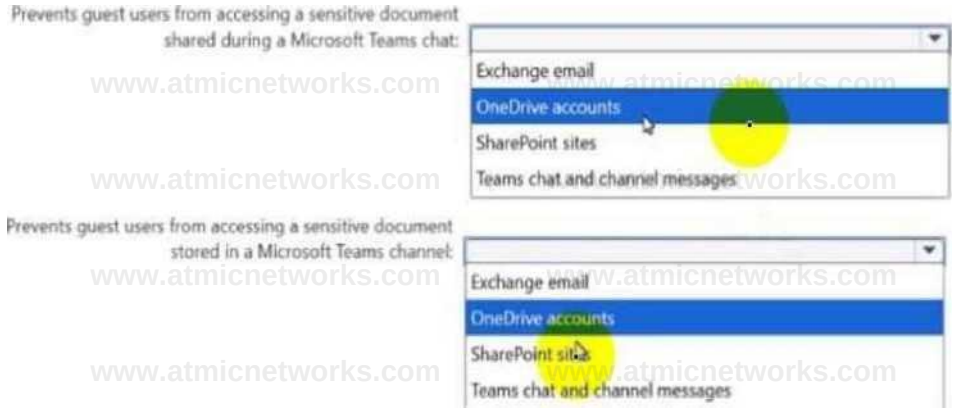
Question: 80

HOTSPOT

You create a data loss prevention (DIP) policy that meets the following requirements:

- Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat
- Prevents guest users from accessing a sensitive document stored in a Microsoft Team? channel Which location should you select for each requirement? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer ATM



Answer:

Explanation:

Answer ATM

Prevents guest users from Accessing a sensitive document shared during a Microsoft Teams chat: OneDnve accounts

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel: SharePoint sites

Question: 81

HOTSPOT

You have a Microsoft 365 ES subscription that uses Microsoft Teams and contains the users shown in the following table.

Name	Team membership
Usefl	Teaml. team?
User 2	Team?

You have the retention policies shown in the following table.

Mame	lotion	Included	Retain items for	Start retention peood	At the end of retention penod
Policy!	Microsoft Teams channel messages Microsoft learns chats	All teams Uteri	7 yews	When items are created	Delete items automatically
Policy?	Microsoft Teams channel messages Microsoft Teams chats	Teamt User?	5 ye#s	When items are created	Delete items automatically

The users perform the actions shown in the following table.

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

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

NOTE: Each correct selection is worth one point

Answer ATM

Statements	Yes	No
I he message edited by Useri will be deleted alter five years		
Uteri can see the message sent by User? for up to seven years		
The message deleted by User 1 will be moved to the SubstrateHolds folder C		

Answer:

Explanation:

Answer Area

Statements	Yes	No
The message edited by User 1 will be deleted alter five years	0	*
Useri can see the message sent by User? tor up to seven years	•	O
The message deleted by Uteri will be moved to the SubstrateHolds folder *		

Question: 82

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

Explanation:

Question: 83

HOTSPOT

You have the files shown in the following table.

Name	Location	Date modified	Date created
RIe1	Microsoft SharePoint Online site	June 01. 2022	December 28. 2015
RIe2	Microsoft OneDrive account	February 02, 2021	January 02.2015
hie 3	Microsoft Exchange Online public folder	May 01 2010	May 01.2010

You configure a retention policy as shown >n the exhibit. (Click the Exhibit lab.)

The start of the retention period is based on when items are created. The current date is January 01. 207S.

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

Answer Atm

Statements	Yes	No
Filet will be deleted alter you turn on the policy		
file? will be deleted after you turn on the policy		
File3 will be deleted after you turn on the policy		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Filet will be deleted alter you turn on the policy		
File? will be deleted after you turn on the policy		
Files will be deleted after you turn on the policy		O •

Question: 84

You have a Microsoft J65 ES subscription.

You need to create a Microsoft Defender for Cloud Apps policy that will detect data loss prevention (DIP) violations. What should you create?

A. a file policy
B. an activity policy
C. a session policy
D. an access policy

Answer: A

Explanation:

Question: 85

HOTSPOT

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	Use* type
U»«1	Member
[Uw2	Guett _____]

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 Bl files, and meeting invites LeamjDQifijslMiuLaCJ^^

O Remove access control settings if already appbed to items

• Configure access control settings

0 Turn on co-au#iomg tor Office desktop apps so multiple users can simultaneously KM labeled documents that have access central settings appiwd. LMnLHSiObatJBMajIS

&

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	Permission* EdR Delete
LegalTeam@86s40q.onmicrosoft.com	Co-Author ^ §
US5ales@86s40q.onmicrosoft.com	

| Use dynamic watermarking O

j Use Double Key Encryption 0

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

Yes No

Only users at yout company can view an email that has the sensitivity label applied.

The owner ol an email can assign permissions when applying the sensitivity label

USSales@86s40qonmicrosolt com can print an email that has the sensitivity label applied

Answer:

Explanation:

Answer Area

Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied	O	•
The owner of an email can assign permissions when applying the sensitivity label	0	•
USSales@86s40q onmicrosoft.com can print an email that has the sensitivity label applied	O	•

Question: 86

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

Nam*	Platform	Microsoft Purview	Microsoft Purview client
Devicel	Windows 11	Not onboarded	Installed
Dev.ce2	Windows 10	Onboarded	Installed
MvVICv J	macOS	Onboarded	Not installed

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

A. Device only
B. Device2 only
C. Device1 and Device2 only
D. Device2 and Device3 only
E. Device1, Device2 and Device3

Answer: B

Explanation:

Question: 87

HOTSPOT

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

Name	Platform
Otvktl	Windows 11
Device	Window; 10
Devices	
| Deviced	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 Area

Answer:

Explanation:

Answer Area

CK Devicel only

To prepare Onboard the rosoft Purview and install the Microsoft Purv*

Question: 88

You have a Microsoft 365 ES subscription.
A security manager receives an email message every time a data loss prevention (DIP) policy match occurs.
You need to limit alert notifications to actionable DLP events. What should you do?

A. From the Microsoft Defender portal, apply a filter to the alerts.
B. From the Microsoft Purview portal, modify the Policy Tips settings of a DLP policy.
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: C

Explanation:

Question: 89

DRAG DROP
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:

Question: 90

HOTSPOT

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Question: 91

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 Administrator
B. Security Reader
C. Security Operator
D. Compliance Data Administrator

Answer: A

Explanation:

Question: 92

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: D

Explanation:

Question: 93

You have a Microsoft $65 subscription.

You plan to retain the following audit log record types and activities for the next three years.

- CopilotInteraction: All activities selected (1/1)

o Interacted with Copilot

- Compliance DLP endpoint: All activities selected {2/2)

o Matched DIP rule

o Removed Dl P rule from document

- AzureActiveDirectory 2 of 25 activities selected (2/25)

o Reset user password o 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: C

Explanation:

Question: 94

You have a Microsoft 565 E5 subscription.
You plan to use Microsoft Purview insider risk management.
You need to create an insider risk management policy that will detect data theft from Microsoft SharePoint

Online by users that submitted their resignation or are near their employment termination date.
What should you do first?

A. Configure a HR data connector.
B. Configure Office indicators.
C. Configure a Physical badging connector.
D. Onboard devices to Microsoft Defender for Endpoint.

Answer: A

Explanation:

Question: 95

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 Security Reader role in the Microsoft Entra admin center
B. the Compliance Management role in the Exchange 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

Explanation:

Question: 96

HOTSPOT
You have a Microsoft 36S ES subscription.
From the Microsoft Purview Data Security Posture Management for AI portal, you review the recommendations for AI data security
You plan to create a one-click policy to block elevated risk users from pasting or uploading sensitive data to AI 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 ATM

I hr policy mode will be configured to me: *

- Tert out first
- Turn it on right away
- Keep it off

The policy will apply to _____

- Devices only
- SharePoint sites only
- Instances only Devices and SharePoint sites
- Devices. Instances, and SharePoint sites

Answer:

Explanation:

Answer Area

The policy mode will be configured to use Test it out first

The policy will apply to; Devices. Instances, and SharePoint sites

Question: 97

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 AI (DSPM for AI).

You need to ensure that User1 can analyze prompts and responses for AI 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: C, E

Explanation:

Question: 98

HOTSPOT

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.

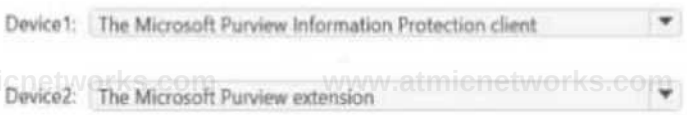
NOTE: Each correct selection is worth one point.

Answer Area

Answer

Explanation:

Answer Area



Question: 99

You have a Microsoft S65 E5 subscription that contains two users named User! and Admin1 Admin1 manages audit retention policies for the subscription.

You need to ensure that the audit logs of User1 will be retained for 10 years.

What should you do first?

A. Assign a Microsoft Purview Audit (Premium) add on license to User1.
B. Assign a 10 year audit log retention add-on license to Admin1.
C. Assign a 10-year audit log retention add-on license to User1.
D. Assign a Microsoft Purview Audit (Premium) add-on license to Admin1.

Answer: C

Explanation:

Question: 100

HOTSPOT

You have a Microsoft 36S ES subscription.

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

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

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

appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer ATN

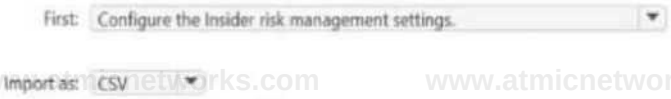
XMI

OPS

Answer

Explanation:

Answer Area



Question: 101

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
File!	
File?	3

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

Name	Content contams	Polky tip	If match, stop pressing	Priority
Rule '	1 or more IP addresses	Tipi	No	0
Rule?	3 or more IP addresses	Tip?	Yes	1
Rule]	2 or more IP addresses	Tipi	No	

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: B

Explanation:

Question: 102

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: B

Explanation:

Question: 103

HOTSPOT

You have a Microsoft 365 tenant

You need to create a new sensitive into 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 m the answer area

NOTE: Each correct selection is worth one point

Answer Area

Primar

Functions

A keyword list

A regular expression

ondary element

Functions

A keyword list

Answer:

Explanation:

Answer Area

Primary element A regular expression

Secondary element A keyword list

Question: 104

You have a Microsoft 565 subscription that contains 100 users and a Microsoft 365 group named Group1. All users have Windows 11 devices and use Microsoft SharePoint Online and Exchange Online. A sensitivity label named Label! is published as the default label for Group1. You add two sublabels named Sublabel1 and Sublabel2 lo Label1. You need to ensure that the settings in Sublabel 1 are applied by default to Group 1. What should you do?

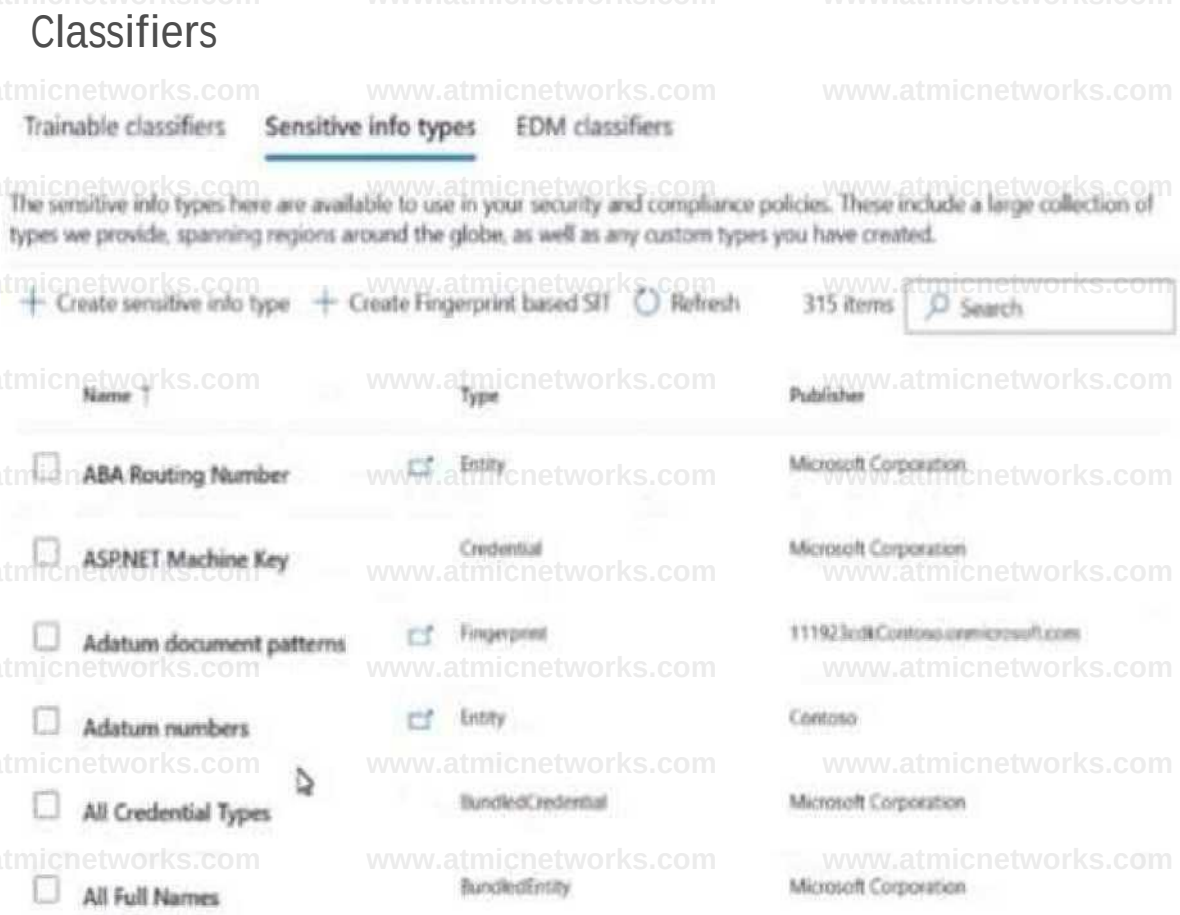
A. Change the order of Sublabel!
B. Duplicate all the settings from Sublabel! to Label1.
C. Modify the policy of Label1.
D. Delete the policy of Label1 and publish Sublabel1.

Answer: C

Explanation:

Question: 105

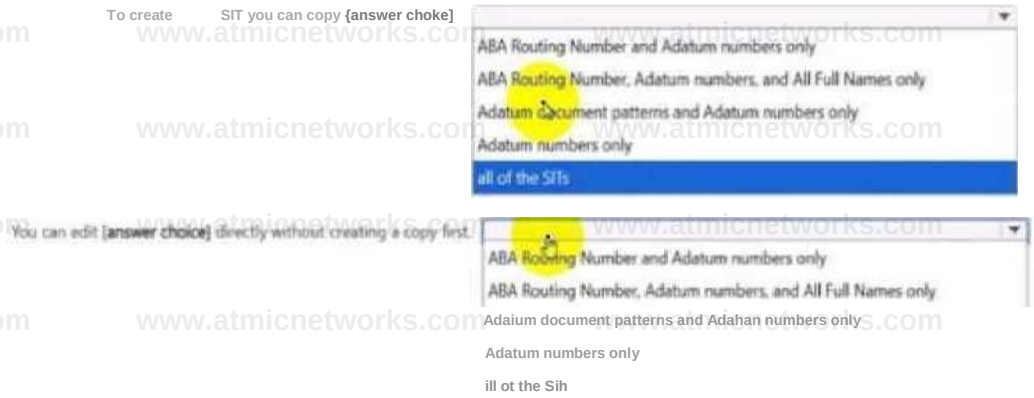
HOTSPOT
You have a Microsoft 36S subscription that contains the sensitive information types (SITs) shown in the following exhibit.



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 flection is worth one point.

Answer Ana



Answer

Explanation:

Answer Area

Question: 106

HOTSPOT

You have two Microsoft 365 subscriptions named Contoso and Fabrikam. The subscriptions contain the users shown in the following table.

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

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

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 Arae Statement! Vet

Uwl can edit ngMt tar hit 1

User? can edit nghu tor F* J Diet 3 can pint Ale2

Answer:

Explanation:

Answer Axe*

Statements	Yes	No

Used can edit rights lor Filet O *

User? can edit rights for File?. O *

User? can print file? O ■

Question: 107

HOTSPOT

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 Area

Devices;

- Devicel only
- Device 1 and Device? only
- Devicel and Device? only
- Device! Device?, and Device?

Use

- File IxplorM
- Microsoft Word
- The Microsoft Defender portal
- The Microsoft Purview portal
- The Settings app

Answer:

Explanation:

Answer Area

Devices Devicel and Device? only *

Use. File (noloter

Question: 108

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.

A user named User 1 sends link based, branded emails that are encrypted by using Microsoft Purview Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients Can User1 revoke the emails?

A. Recipient1 only
B. Recipient4 only
C. Reciptent1 and Recipient^ only
D. Reclpient3 and Recipients only
E. Reciptent1, Recipient2. Recipient3, and Recipient4

Answer: D

Explanation:

Question: 109

HOTSPOT

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 Area

All email to a domain named fabrikam.com must be encrypted automatically:
- A data connector in the Microsoft Purview portal
- A data loss prevention (DLP) policy in the Microsoft Purview portal
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:
- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft Purview portal
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft Purview portal

Answer:

Explanation:

AnMer Arm

All enrol So A tawi named tjarkam com must be A nut Bow rule n the hrhange admm center encrypted automacxGeHv

Encrypted email meat e^ve seven days after they er rent A custom bcandnq temptate in Merosoh Exchange Online Pcwe<Shel

Question: 110

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: B

Explanation:

Question: 111

HOTSPOT

You have a Microsoft 36S subscription.

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

Protect with OMEv2

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.

l»«W*rt

mu# *OR m to tfw Qfct M MHMM t-m

mvwgm (>rrw»tRl •utomrtxji

FRt» |•W^^>W•1

Answer:

Explanation:

*4f, port#

Question: 112

You have a Microsoft 36S ES subscription

You plan to create an met data match (EDM) classifier named EDM1.

You need to grant permissions to hash and upload the sensitive ^formation source table for EDMI. What should you create first?

A. a Microsoft Entra enterprise application named EDM.DataUploaders
B. a Microsoft Purview role group named EDM.DataUploaders
C. a security group named EDM.DataUploaders
D. a Microsoft Entra app registration named EDM.DataUploaders
E. a Microsoft 365 group named EDM.Datauploaders

Answer: C

Explanation:

Question: 113

HOTSPOT

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	Ws	No
Uteri cm apply Labeil Io file 1 png by using the information protection client	O	O

Uteri cm apply LabeH to Folder? by using the information protection client

User? cm apply Label 1 to hie? dot* by usmg the information protection client. 0 O

Answer:

Explanation:

Answer Am

Statements	Wt	No
chert can apply UteH to Filet.png by using the irdormatron protection chent	0	
Uwrt can apply labell to Folder? by using the intamatton protection client	0	•
Cher? can apply Labeit to File? doa by usmg the information protection client	•	O

Question: 114

You are creating a custom trainable classifier to Identify organizational product codes referenced in Microsoft 36S content. You identify 300 files to use as seed content When? should you store the seed content?

A. a Microsoft OneDrive folder
B. a Microsoft Exchange Online shared mailbox
C. an Azure file share
D. a Microsoft SharePoint Online folder

Answer: D

Explanation:

Question: 115

You have a Microsoft 365 ES 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 hearth service numbers from the UK
- Sensitive projects that contain the following words: Project Tailspin. Project Contoso, and Project falcon

You have email messages m 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

Explanation:

Question: 116

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: B

Explanation:

Question: 117

HOTSPOT

You have a Microsoft 36515 subscription tha1 contains a Microsoft SharePoint Online site named Site1 Site1 contains three tiles named File1. File2 and File3.

You create the data loss prevention (DIP) policies shown in the following table.

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

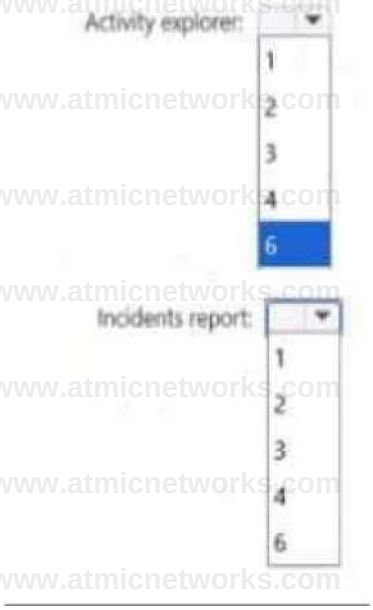
The DIP rule matches for each tile are shown in the following table.

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

How many DIP policy matches events will be added to Activity explorer, and how many policy matches will be added to the DLP incidents report? To answer, select the appropriate options m the

answer area.

Answer Area



Answer:

Explanation:

Activity explorer= 6
Incidents report= 4
Answer Am

Incidents report:

Question: 118

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. Yes
B. No

Answer: A

Explanation:

Question: 119

You implement Microsoft 36S Endpoint data loss pi event ion (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 onboard the computers to Microsoft Defender for Endpoint Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Question: 120

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. Yes
C. No

Answer: A

Explanation:

Question: 121

You implement Microsoft 36S Endpoint data loss pi event ion (Endpoint DIP).
You have computer 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 Microsoft Purview Information Protection client to the computers.
Does this meet the goal?

A. Yes
D. Yes

Answer: B

Explanation:

Question: 122

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

Naw	Authenticated users View contenifVIEW)	Authenticated users Copy and ertract c orrtent (EXTRACT)	Authenticated users Export conientfEXPORT)
label'	Granted	Not granted	Not granted
label?	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: A

Explanation:

Question: 123

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. Information Protection
B. Information Barriers
C. Insider Risk Management
D. Data Loss Prevention

Answer: D

Explanation:

Question: 124

You have a Microsoft 365 E5 subscription that contains a user named User1.
You deploy Microsoft Purview insider risk management.
You need ensure that insider risk management events related to User1 are visible only to specific users.
What should you create?

A. a global exclusion
B. an indicator variant
C. a priority user group
D. a detection group

Answer: D

Explanation:

Question: 125

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

Explanation:

Question: 126

HOTSPOT
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 area.
NOTE: Each correct selection is worth one point.

Answer Area

Credit card numbers I Data Loss Prevention *]

Communication Compliance
Data Loss Prevention
Information Barriers
Insider Risk Management

Documents Data Loss Prevention

Communication Compliance

Data loss Prevention

Information Barriers

Insider Risk Management

Answer:

Explanation:

Answer Area

Credit card numbers: Data Loss Prevention

Documents Data loss Prevention

Question: 127

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

You are evaluating the use of custom data assessment scans to identify the potential oversharing of data in the subscription.

What is the maximum number of items the data assessments can support per location?

A. 50.000
B. 100.000
C. 200.000
D. 500.000

Answer: C

Explanation:

Question: 128

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

Explanation:

Question: 129

You have a Microsoft 365 E5 subscription that has a sensitivity label named Sensitivity1.

You plan to create an auto-labeling policy that will apply Sensitivity1 to Microsoft Exchange Online mailboxes.

On February 1, you create the auto-labeling policy and enable simulation mode by using the default settings. No modifications are made to the policy in simulation mode.
When will the policy first be turned on?

A. February 2
B. February 6
C. February 15
D. never

Answer: C

Explanation:

Question: 130

You have a Microsoft 36S E5 subscription that has a Microsoft Purview exact data match (EDM) classifier named EDM1.
You plan to create the Microsoft Purview policies shown in the following table.

Name	
DLP1	Data loss prevention (DLP)
Insidefl	Insider risk management
Retention 1	Retention

Which policies can use EDM1?

A. DLP1 only
B. Retention 1 only
C. DLP1 and Insider1 only
D. Insider1 and Retention1 only
E. DLP1. Insider1, and Retention1

Answer: A

Explanation:

Question: 131

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: B, G

Explanation:

Question: 132

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
FileI.docx	Useri
Fileldoa	User?
FBe3.doc*	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: B

Explanation:

Question: 133

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: D

Explanation:

Question: 134

HOTSPOT

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.

Assign permissions to specific users and groups *

Assign permissions

4 items

Users and groups	Permissions	Edit	Delete
U5er1@86s40q.onmicrosoft.com	Co-Owner	^	[jj
Usef2®86s40q.onrnrcrosoflcom	Co-Author	^	[J]
usef3@S6s40q.onmicrosoft.com	Reviewer	^	g
U5er4@86s40q,onmicrosoft, com	Viewer		0

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, User2, User3, and User4

- 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, User2, User3, and User4

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

Answer

Explanation:

Answer Area

Microsoft 365 Copilot can summarize Riel for [answer choice] User], Usetz. Userl and User4

For [answer choice] Microsoft 365 Copilot can reference File 1 by using a link User!, Userz, Userl and User-1

Question: 135

HOTSPOT

You have a Microsoft 365 £5 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

Use the Microsoft Purview portal

| Microsoft 365 admin center

Microsoft Defender portal Microsoft Enna admin center

Microsoft Purview portal

Format in: HTML

HI ML

Markdown

RTF

XML

Answer:

Explanation:

Answer Area

Use the: Microsoft Purview portal

Forma! in HTML

Question: 136

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. The subscription contains an Endpoint data loss prevention (Endpoint DLP) policy as shown in the Actions exhibit. (Click the Actions tab.)

^ **Actions**

Use actions to protect content when the conditions are met

^ **Audit or restrict activities on devices**

When specific activities are detected on devices with protected files containing sensitive information, you can choose whether to only audit the activity block it entirely, or block it and allow users to overnde the restnction.
Learn more restricting device activity

Service domain and browser activities
Detects when protected files are blocked or allowed to be uploaded to doud service domains based on the Allow/Block doud service domains' list in endpoint DLP settings.

a Upload to a restricted doud service domain or access from an unallowed browsers	0	Audit only
Sensitive service domain group restnebonfs) configured. Edit		
Q Paste to supported browsers	0	Audit only
Sensitive service domain group restriction's) configured. Edit		

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

Sensitive service domain restrictions
Erfc«e difereet retire! or* tot seo five sen ice dor an that are def red by the totitive service coma n groups set up in endpoint DLP settings

+ **Add group**

Group	Priority	Action
j %<XJ 5«fV£K	1	S ock with ov„
j *V« Swene	2	Shock
Ll Generative A webiires	3	Seek

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

Sensitive service domain restrictions

Enforce different restrictions for sensitive service domain groups set up in endpoint DLP settings.

| Add group

Group	Priority	Action
Mail Sermces	1	Block
Geneeaive Ai Webster	2	Block with ov..

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

(■ Q 1itps7rchatgpt.com

0 Microsoft Purview Data Loss Prevention

Von have attempted an unauthorized action.

ChatGr you | we attempted an unauthorized action which involved sensitive data. You actions will be Explore logged.

DIvnM

2023

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
Used can paste sensitive data from an email to ChatGPT after selecting Dismiss.		
Useri can upload emails that contain sensitive data to ChatGPT after selecting Dismiss.		
Useri can paste sensitive data from a Microsoft Word document to ChatGPT after selecting Dismiss		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can paste sensitive data from an email to ChatGPT after selecting Dismiss.	0	t
Useri can upload emails that contain sensitive data to ChatGPT after selecting Dismiss.		•

Useri can paste sensitive data from a Microsoft Word document to ChatGPT after selecting
Dismiss

Question: 137

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview Audit (Premium) with the 10-Year Audit Log Retention add-on license.

The subscription contains the audit retention policies shown in the following table.

Name	Users	Record type	Activities	Duration	Priority
RP1	User 1	SharePoint	Created site collection	1 Year	30
RP2	User!	SharePoint	*None*	3 Years	20
RP3	Useri	SharePoint	Created site collection		40
RP4	Useri	SharePoint	Renamed site	6 Months	10

From the SharePoint Online admin center, User1 performs the actions shown in the following table.

Name	Description
ActionI	Archives a site
Action?	Creates a site collection
Actions	Renames a site

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
ActionI will be retained for one year.		
Action? will be retained for three years.		
Actions will be retained for six months.		

Answer:

Explanation:

Answer Area Statements	Yes	No
ActionI will be retained for one year.	O	•
Action? will be retained for three years,		•
Actions will be retained for six months.	•	

Question: 138

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: C

Explanation:

Question: 139

You have a Microsoft 365 E5 subscription.

You plan to use insider risk management to collect and investigate forensic evidence.

You need to enable forensic evidence capturing.

What should you do first?

A. Configure the information protection scanner.
B. Claim capacity.
C. Enable Adaptive Protection.
D. Create priority user groups.

Answer: B

Explanation:

Question: 140

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. Create a data loss prevention (DLP) policy.
B. Turn on Indicators.
C. Configure adaptive protection.
D. Turn on analytics.
E. Create an insider risk policy.

Answer: B, E

Explanation:

Question: 141

You have a Microsoft 365 subscription.
You create and run a content search from the Microsoft Purview portal.
You need to download the results of the content search.
What should you obtain first?

A. a certificate
B. a password
C. a pin
D. an export key

Answer: D

Explanation:

Question: 142

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

Name	Role
Useri	Owner
User2	Member

You create the retention labels shown in the following table.

Name	Retention period	Retention action	Based on
Retention 1	4 years	Retain only	When a file was labeled
Retentions	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
Filel	Useri	Retention 1
File2	Useri	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 Area

Statements	Yes	No
Useri can delete Filel on March 10.2023.	O	O
User2 can delete Filel on March 10.2027.	O	O
User2 can edit File2 on March 15,2025.	O	O

Answer:

Explanation:
Answer Area

Statements	Yes	No
User! can delete Filel on March 10,2023.	O	<•'
User2 can delete Filel on March 10.2027.	O	#
User2 can edit File2 on March 15, 2025.	O	•

Question: 143

HOTSPOT
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 Area

Create Sensitive 1 by using: The Microsoft Purview portal Security & Compliance PowerShell

The Exchange admin center

The Microsoft Purview portal

The SharePoint admin center

Use Sensitivel in: DLP1, DLP2 and DLP3 ▼

DLP1 only

DLP2 only

DLP1 and DLP2 only

DIPT DLPZ and DLP3

Answer:

Explanation:

Answer Area

Create Sensitivel by using: The Microsoft Purview portal

Use Sensitivel in: DLP1, DLP2, and DLP3

Question: 144

HOTSPOT

You have a Microsoft 365 E5 tenant.

You have sensitivity labels as shown in the Sensitivity Labels exhibit. (Click the Sensitivity Labels tab.)

4* Create a label £3 Publish labels Q Refresh

Name		Order	Stope
Public		0 - lowest	Fi e Emal
General			fie Email
Confidential	—	2	fie Email
Internal	...	3	fi e Email
External		4 - hgheit	file Email

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.)

Sensitivity Policyl

Edit policy 0 Delete polity

Name

Sensitivity Policyl

Description

Published labels

Public
General
Confidential
Ccrfidential/Intema:
Ccnfidential/External

Published to
All

Policy settings
Users must provide justification to remove a label or lower its classification

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

Answer Area

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

Answer:

Explanation:

Answer Area

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

Question: 145

You have a Microsoft 365 subscription.
You create a new trainable classifier.
You need to train the classifier.
Which source can you use to train the classifier?

A. an on-premises Microsoft SharePoint Server site
B. an A2ure Files share
C. a Microsoft SharePoint Online site
D. an NFS file share

Answer: C

Explanation:

Question: 146

You have a Microsoft 365 tenant that uses Microsoft Purview Message Encryption.
You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using Microsoft Purview Message Encryption.
What should you do?

A. From the Exchange admin center, create a mail flow rule.
B. From the Exchange admin center, create a new sharing policy.
C. From the Microsoft Defender portal, create a Safe Attachments policy.
D. From the Microsoft Purview portal, configure an auto-apply retention label policy.

Answer: A

Explanation:

Question: 147

HOTSPOT
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.)

Edit sensitivity label

- Q Label details
- Q Scope
- O Items
- O Groups & sites
- 0 Schematized data assets (preview)
- 0 Finish

Review your settings and finish

Name

Contoso Confidential

Display name

Contoso Confidential

Edit

Description for users

Contoso Confidential

Edit

Scope

Files & other data assets, Email

£&i

Access control

Edit

Content marking

Footer Contoso Confidential Internal use only

Lilt

Auto labeling for files and emails

None

Litt

Auto-labeling for schematized data assets (preview)

None

Edit

Save label

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

Edit sensitivity label

0 Label details

0 Scope

Q Items

0 Groups & sites

9 Schematized data assets (preview)

• Finish

Review your settings and finish

Name

Contoso Confidential

Display name

Contoso Confidential

Esta

Description for users Contoso Confidential

Edit

Scope

Files & other data assets. Email

Edit

Access control

Access control

Etta

Content marking

Footer Contoso Confidential Internal use only

Edit

Auto labeling for files and emails

None

Edit

Auto-labeling for schematized data assets (preview)

None

Esta

Back Cancel

Edit sensitivity label

O Label details

Q Scope

9 **Items**

• **Access control**

O Content matting

o Auto-tateUng tot flies and
I emails

O Groups & sites

O Schematized data assets
| (prevrewi

0 finish

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 mote about access cooiroLsfiitags

0 Remove access control settings if already applied to items

® Configure access control settings

HI **Turn on co-authoring tor Office desktop apps so multiple users can simultaneously edit UMM documents mat have access Control settings applied ri ' mr-. itcud :** letting

[Go to co authoring setting 1

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 0

Never

Allow offline access 0

Only for a number of days

Users have offline access to the content foi this many days

Assign permissions to specific users and groups '

Assign permissions

11tem

Users and groups	Permissions Edit Delete
authertKatMUsers	Co-Author ^ @

2] Use dynamic watermarking O

^ Use Double Key Encryption O

Next I

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

Answer Area

Statements	Yes	No
if a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential	○	○
Guest users will be able to open documents protected by Contoso Confidential	○	○
Contoso Confidential will be applied automatically to rhe files stereo in Microsoft SharePoint Online	○	○

Answer:

Explanation:

Answer Area

Statements	Yes	No
if 3 user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential	●	○
Guest users will be able to open documents protected by Contoso Confidential	○	●
Contoso Confidential will be applied automatically to the files stereo in Microsoft SharePoint Online	○	●

Question: 148

HOTSPOT
You have a Microsoft 365 £5 subscription.
You have a Microsoft Purview Advanced Message Encryption branding template named 0ME1.
You need to create a Microsoft Exchange Online mail flow rule to apply OME1 to email.
How should you configure the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

To apply custom banding to 0ME1 messages:

Apply this rule if: The sender | Is external/internal

The sender
A message header The
message properties
The recipient

Is external/internal
Contains any of these sensitive info types
Has specific properties including any of these
Includes the classification
Includes the importance level
Is extemal/internai

Modify the message secutity.

Apply a disclaimer to the message. Modify the message properties
Modify the message security.
Redirect the message

Answer:

Explanation:

Answer Area

Apply this rule it The sender ' Is external/internal

To apply custom branding to 0ME1 messages: Modify the message security. '

Question: 149

You have a sensitive information type based on a trainable classifier.
You are unsatisfied with the result of the trainable classifier.
You need to retrain the classifier.
What should you use in the Microsoft Purview portal?

A. Content explorer from Data classification
B. Labels from Information protection
C. Labels from Information governance
D. Content search

Answer: A

Explanation:

Question: 150

HOTSPOT
You have a Microsoft 365 £5 subscription that contains the groups shown in the following table.

Name	Type	Primary email address
Group!	Microsoft 365	Group 1 @cont oso.com
De."	Distribution	Dtst1@contoso.com

The subscription contains the users shown in the following table.

Name	Member of
Userl	Group!
User?	Dist!
User3	*None*

You create the mail flow rules shown in the following table.

Name	Apply this rule if	Do the following
	. The recipient is a member of Rule! group! ©contoso.com	Apply Office 365 Message Encryption and rights protection
	„ . , The sender is Rule? . * dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

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

Answer Area

Statements	Yes	No

If U$er2 sends an email message	to User3, the message is encrypted automatically,	O	<.1
If User2 sends an email message	to Useri, the message is encrypted automatically.	O	O

If User 3 sends an email message to Group 1, the message delivered to Used is encrypted automatically.

Answer:

Explanation:

Answer Area

Statements	Yes	No
If User? sends an email message to User3, the message is encrypted automatically,	#	■
If User? sends an email message to Useri, the message is encrypted automatically.	•	
If User? sends an email message to Groupl, the message delivered to Useri is encrypted automatically.		•

Question: 151

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: C

Explanation:

Question: 152

You have a Microsoft 365 E5 subscription.

You create a sensitivity label named Label1 and publish Label1 to all users and groups.

You have the following files in a SharePoint site:

- File1.doc
- File2.docx
- File3.xlsx
- File4.txt

You need to identify which files can have Label1 applied. Which files should you identify?

A. File2.docx only
B. File2.docx and File3.xlsx only

C. File1.doc File2-docx, and File3.xlsx only
D. File1.doc File2-docx, File3.xlsx, and File4.txt

Answer: B

Explanation:

Question: 153

You have a Microsoft 365 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2. You plan to use policies to meet the following requirements:

- Add a watermark of Confidential to a document if the document contains the words Project1 or Project2.
- Retain a document for seven years if the document contains credit card information.
- Add a watermark of Internal Use Only to all the documents stored on Site2.
- Add a watermark of Confidential to all the documents stored on Site1.

You need to recommend the minimum number of sensitive info types required.

How many sensitive info types should you recommend?

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

Answer: C

Explanation:

Question: 154

You need to test Microsoft Purview Advanced Message Encryption capabilities for your company. The test must verify the following information:

- The acquired default template names
- The encryption and decryption verification status

Which PowerShell cmdlet should you run?

A. Test-OAuthConnectivity
B. Test-ClientAccessRule
C. Test-IRMConfiguration
D. Test-Mailflow

Answer: C

Explanation:

Question: 155

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

Name	Type	Query
Scopel	Users	FirstName starts with User
Scope?	SharePoint Online sites	SiteTitle starts with Site

You create the retention policies shown in the following table.

Name	Type	Location
RPolicyl	Adaptive	Scopel
R Policy?	Adaptive	Scopel
RPolicy3	Static	Microsoft 365 groups

Which retention policies support a preservation lock?

A. RPolicy2only
B. RPolicy3on1y
C. RPolicy1 and RPolicy2 only
D. RPolicy1 and RPolicy3 only
E. RPolicy1, RPolicy2, and RPolicy3

Answer: B

Explanation:

Question: 156

At the end of a project, you upload project documents to a Microsoft SharePoint Online library that contains many files. The following is a sample of the project document file names:

- aei_AA989.docx
- bd_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx
- ecc_BB565.docx

All documents that use this naming format must be labeled as Project Documents:

You need to create an auto-apply retention label policy.

What should you use to identify the files?

A. A retention label
B. A trainable classifier
C. A sensitive info type

Answer: C

Explanation:

Question: 157

DRAG DROP

You have a Microsoft 365 £5 subscription.

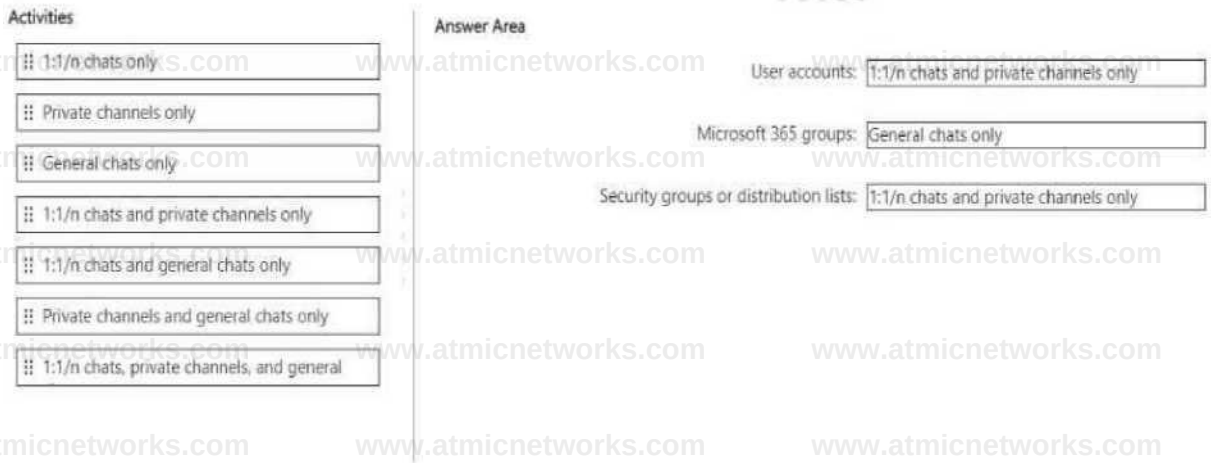
You need to prevent the sharing of sensitive information in Microsoft Teams.

Which entities can you protect by applying a data loss prevention (DLP) policy to each resource? To answer, drag the appropriate activities to the correct entity. Each activity 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:

Question: 158



You have a Microsoft 365 E5 subscription.

You create a data loss prevention (DLP) policy and select.

Use Notifications to inform your users and help educate them on the proper use of sensitive info.

Which apps will show the policy tip?

A. Outlook on the web only

B. Outlook Win32 only
C. Outlook for iOS and Android only
D. Outlook on the web and Outlook Win32 only
E. Outlook Win32 and Outlook for iOS and Android only
F. Outlook on the web. Outlook Win32, and Outlook for iOS and Android

Answer: D

Explanation:

Question: 159

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

Policy1 contains an advanced data loss prevention (DLP) rule named Rule1.
Which two conditions can you use in Rule1? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Document property is
B. Attachment's file extension is
C. Document size equals or is greater than
D. Content is shared from Microsoft 365
E. Content contains

Answer: D, E

Explanation:

Question: 160

You have a Microsoft 365 E5 subscription that contains a device named Device1.
You need to enable Endpoint data loss prevention (Endpoint DLP) for Device1.
What should you do first in the Microsoft Purview portal?

A. Turn on device onboarding.
B. Enable Microsoft Priva Privacy Risk Management.
C. Create a Microsoft Purview Information Barriers (IBs) segment.
D. Add a Microsoft Purview Information Protection scanner cluster.
E. Onboard Device1 to Microsoft Purview.

Answer: A

Explanation:

Question: 161

You have a Microsoft 365 E5 tenant.
You create a data loss prevention (DLP) policy.
You need to ensure that the policy protects documents in Microsoft Teams chat sessions.
Which location should you enable in the policy?

A. SharePoint sites
B. Exchange email
C. Teams chat and channel messages
D. OneDrive accounts

Answer: D

Explanation:

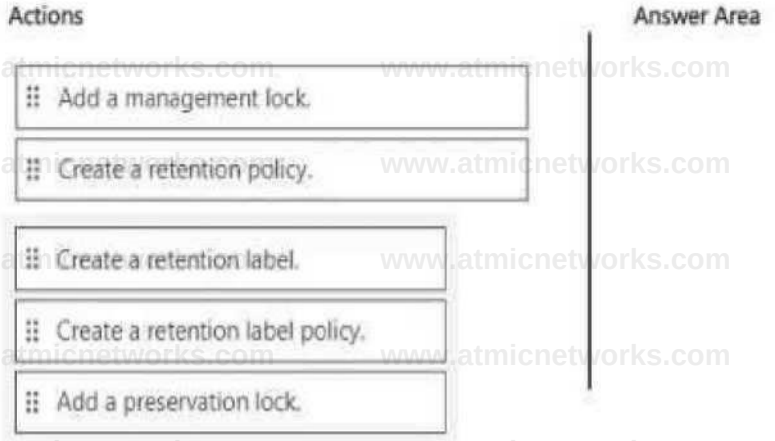
Question: 162

DRAG DROP
You have a Microsoft 365 tenant.
A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years,

and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.

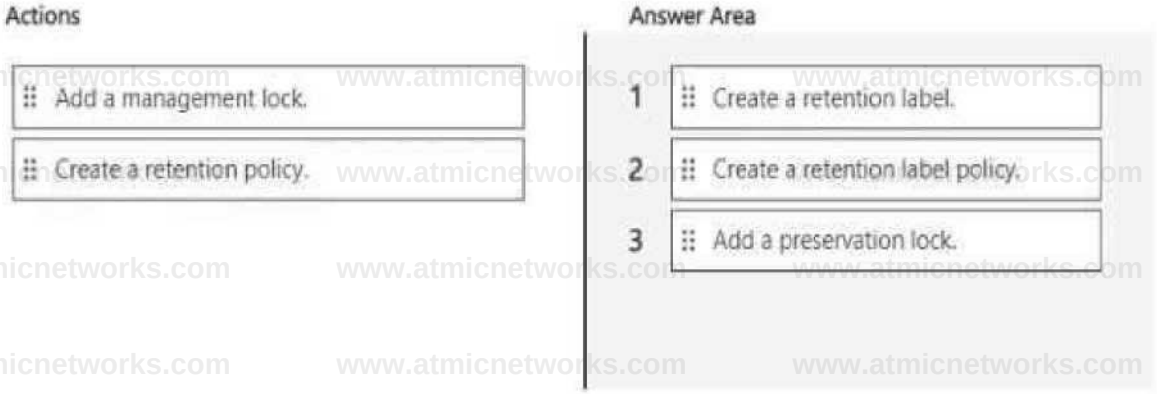
You need to implement the regulatory requirement.

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



Answer:

Explanation:



Question: 163

You need to create a retention policy to delete content after seven years from the following locations:

- Exchange Online email
- SharePoint Online sites
- OneDrive accounts
- Microsoft 365 Groups
- Teams channel messages
- Teams chats

What is the minimum number of retention policies that you should create?

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

Answer: B

Explanation:

Question: 164

HOTSPOT

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 Area

Answer:

Explanation:

Answer Area

Set-RetentronCompliancePolicy ' id contoso.Policy RetryDistribution '

Question: 165

HOTSPOT

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
Userl	Members group of Sitel
	Owners group of Sitel
Adminl	SharePoint Administrator role

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

Actions

Use actions to protect content when the conditions are met

Restrict access or encrypt the content in Microsoft 365 locations —

| Restrict access or encrypt the content in Microsoft 365 locations

(•) Block users from receiving email or accessing shared SharePoint OneDrive. and Teams files

By default users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting But you can choose who is blocked from rece mg emails or accessing files shared from SharePoint. OneDrive and Teams.

Block everyone. Qj

Q Block onl . people outside your organization.[1] .

Q Block only people who were given access to the content through the 'Anyone with the fink" option. C

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 Area

Statements	Yes	No
Used can access Filel on Srtel.	0	
UserZ can access Filel on Site!		
Admin! can access Filel on Site!.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Us^rl can access Fllel on Sitel.	0	0
User? can access Filel on Site!	A	
Admin 1 can access Filel on Sitel		

Question: 166

HOTSPOT

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

HJTW	Stor'd st	Numt* e* »*T»itiw Intonniifl" ryp« tSIH		
		IP atoms	SWI'Itode	SntrM accesi i*;-s:u'SASI
Ffa1	Microti Uchonot Orfe's		1	4
IM	MHK MI		J	
FtteS	Miero::+t j'	1	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. Amw*' A'W SM»<IMH«3 *• Na

fatrii - it tppbid to Fdel

Fft v."i applied to F 1*2

Ft> • ,■.' H applied to F>3

Answer:

Explanation:

Am**1 AW

SliltMWtI	^#	HQ
Ri!irti>Al b kpplndto F4»l	•	
Retertenl« applied to Rei	♦	

Reteflboni it applied to total

Question: 167

You have a Microsoft 365 E5 subscription that contains a data loss prevention (DLP) policy named DLP1. DLP1 contains the DLP rules shown in the table.

♦#!•	Ft««ty	Jw •or *<r <in*	Policy tap	' tlwe'e • itudtA tor OM ru'd Mop pwtduinp Mtdironal DIP palli I* indium
	0	On	Tip 1	in «i>tad
	1	On		tn ebled
Fuie*	2	On	Tip 3	3ts»bl«d
BiW	I	On	*p4	Enabled

You need to ensure that when a document matches all the rules, users will see Tip 2. What should you change?

A. the priority setting of Rule2 to 0
B. the priority setting of Rule2 to 2
C. the priority setting of Rule3 and Rule4 to 0

D. the If there's a match for this rule, stop processing additional DLP policies and rules setting for Rule3 to Enabled

Answer: A

Explanation:

Question: 168

You have a Microsoft 365 E5 subscription that contains a user named User1. You deploy Microsoft Purview Data Security Posture Management for AD (DSPM for AD). 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. Insider Risk Management Analysts
B. Security Reader
C. Insider Risk Management Investigators
D. View-Only Organization Management for Microsoft Exchange Online

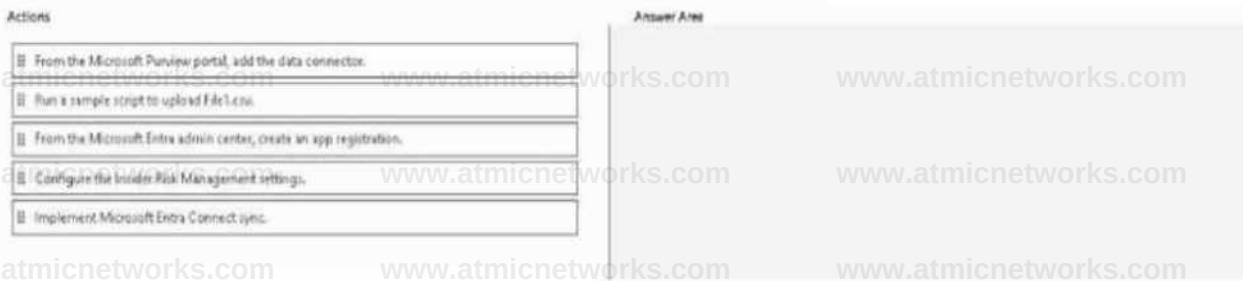
Answer: B

Explanation:

Question: 169

DRAG DROP

You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview Insider Risk Management.
You obtain a file named File1.csv that contains employee resignation data.
You need to implement the HR data connector and upload File1.csv by using the connector.
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:

ACtMJRB

Annver AHM

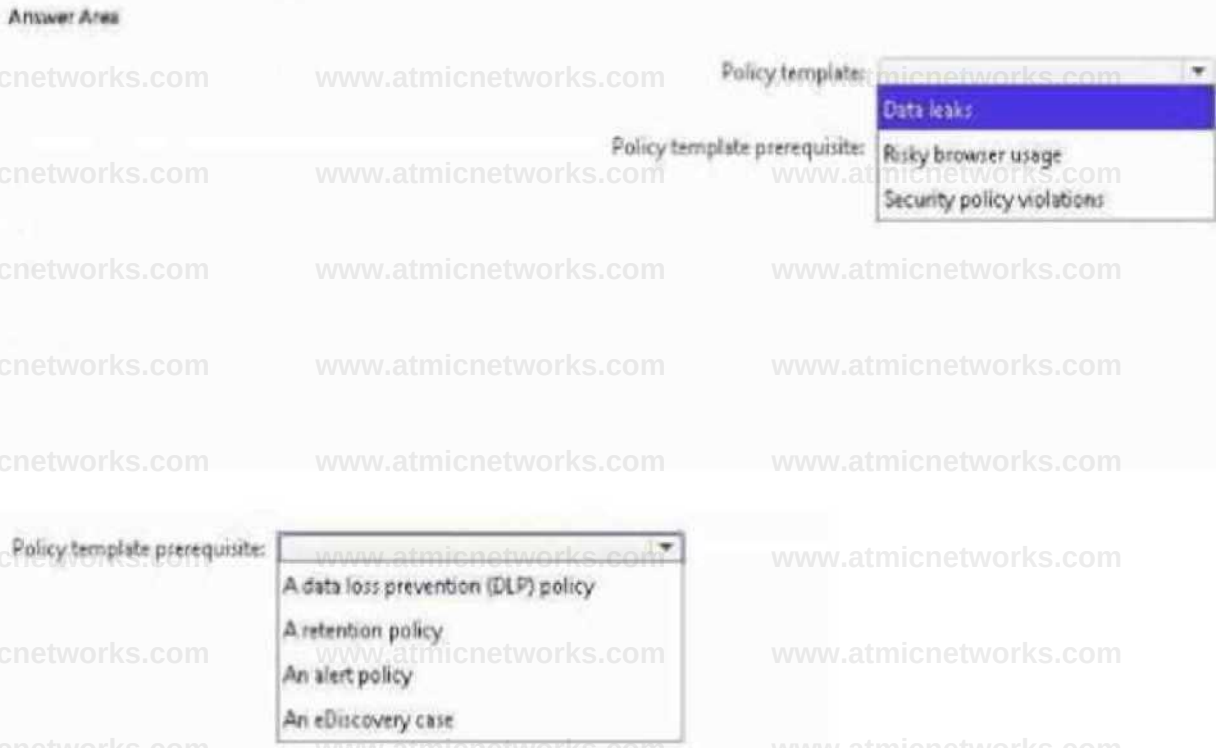
2 C onngufe the ■■ :4« -is! Manic*'-e't usings.

1 2 from the Mfrs i aft Envt admin center create an act* ngcttatior

Question: 170

HOTSPOT

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



Answer:

Explanation:

Aniwr A'*

i'll it y templet DiUkik'

Policy ten*pl«te prerequisite A drip lw prevention (DLP) policy

Question: 171

You have a Microsoft 365 E5 subscription.
You are implementing insider risk management.
You need to maximize the amount of historical data that is collected when an event is triggered.
What is the maximum number of days that historical data can be collected?

A. 30
B. 60
C. 90
D. 180

Answer: C

Explanation:

Question: 172

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. Install the Microsoft Purview extension on the devices.
B. Create a data leaks policy.
C. Onboard the devices to Microsoft Purview.
D. Create a communication compliance policy.
E. Create an Endpoint data loss prevention (Endpoint DLP) policy.
F. Enroll the devices in Microsoft Intune.

Answer: A, C

Explanation:

Question: 173

You have a Microsoft 365 E5 subscription that uses retention label policies.
You need to identify all the changes made to retention labels during the last 30 days.
What should you use in the Microsoft Purview portal?

A. Reports
B. Activity explorer
C. User data search
D. Content search

Answer: B

Explanation:

Question: 174

DRAG DROP
You have a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management and contains three users named User1, User2, and User3.
All insider risk management policies have adaptive protection enabled and the default conditions for insider risk levels configured.
The users perform the following activities, which trigger insider risk policy alerts:
User1 performs at least one data exfiltration activity that results in a high severity risk score.
User2 performs at least three risky user activities within seven days, that each results in a high

severity risk score.

User3 performs at least bwo data exfiltration activities within seven days, that each results in a high severity risk score.

Which insider risk level is assigned to each user? To answer, drag the appropriate levels to the correct users. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or seroll to view content.

NOTE: Each correct selection is worth one point.

Ul«1 , Int>d«r hrt inti

Uiwl imrdir mi it.*1

U><«) ' InnJti m« I,.*'

Answer:

Explanation:

A-iww A<»«

I Id E'4vvt*dfut icwl

J«i Modtnti mt IMI

User3: Moderate risk level

Question: 175

HOTSPOT

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

Name	Microsoft Purview role group	Microsoft 365 role
User1	None	Global Administrator
User2	Insider Risk Management Analysts	None
User3	Insider Risk Management Investigators	None

The subscription contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Microsoft 365

You plan to create a priority user group named Priority1.

You need to identify the following:

. Which users and groups can be added to Priority1?

. Which users can be enabled to view alerts that involve the members of Priority1?

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

Ana** A.W

UMfl •«!/ *Cw* b. HI^M to ww J»i>*a« *—*• *• ■• •^«1 IS'^I u-i1

^0^1 any UMI] mdUivlany UMI) >4 few** «y

fr«Ml «nd&<9u#J any Uwtl Hull an# Um) any UMIl. UMI|

UMI), Orona* wMuioupJ

UMIl any

UMI) any

UMU annum)any

UMI)M4UI«)M^

UM<1 UH4 IMUM*)

Answer:

Explanation:

Amwr Aw

< tn b« «d(>-i ta 9nontyV UIH' Jitrj, Uitr3, Group), and G*oup2

Csn be sntbirl to v*ew «>■'. JhH vokt th* n *rnbtr> if Ptmntyl: 'Jitfi « ■ : U.tfJ uny

Question: 176

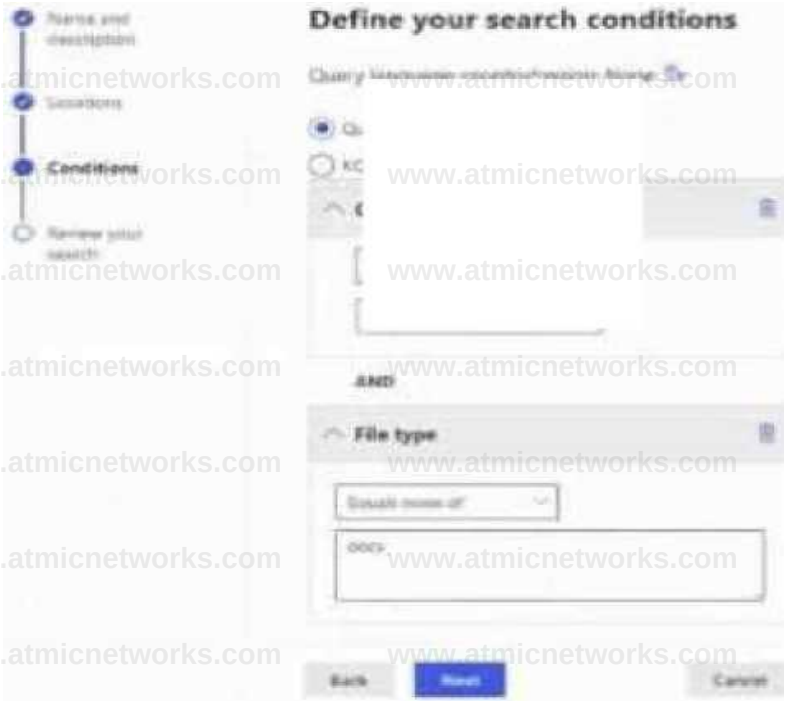
HOTSPOT

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.

Anu*' A^»

jUtMIMHtt Ne

file? n I'xhidesm the Seerchi •- .•»

file) itmchnMi* Hie 'weechi rt.

Answer:

Explanation:

Anu>»'A'W

ftMaowna Hu

Ik , ■

Hr? i! included w the civ ch 1 wail

Question: 177

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains three files named File1, File2, and File3.

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

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

The DLP rule matches for each file are shown in the following table.

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

How many DLP policy matches events will be added to Activity explorer, and how many policy matches will be added to the DLP incidents report? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Question: 178

Nate: 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