

Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365



NEW QUESTION 1

HOTSPOT - (Topic 1)

You are reviewing policies for the SharePoint Online environment.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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.	<input type="checkbox"/>	<input type="checkbox"/>
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.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

AI-generated content may be incorrect. Understanding Site4's Retention Policies:

Site4RetentionPolicy1 deletes items older than 2 years from creation. If a file was created on January 1, 2021, it would be deleted after January 1, 2023.

Site4RetentionPolicy2 retains files for 4 years from creation. If a file was created on January 1, 2021, it will be kept until January 1, 2025, but not deleted after that (policy states "Do nothing").

Statement 1 - Yes, because Site4RetentionPolicy2 ensures files are retained for 4 years. Statement 2 - Yes, because Site4RetentionPolicy2 retains the file for 4 years (until January 1, 2025).

Statement 3 - No, because retention is only for 4 years (until January 1, 2025). After that, the policy does "nothing," meaning the file is no longer recoverable after that period.

NEW QUESTION 2

HOTSPOT - (Topic 1)

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 User1 can access:

Number of files that User2 can access:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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?
File1.docx	1	<input type="checkbox"/> No restriction (SWIFT codes < 2)
File2.bmp	4	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File3.txt	3	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	<input type="checkbox"/> 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?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.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.

NEW QUESTION 3

HOTSPOT - (Topic 1)

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 DLP policy

A sensitive info type

A sensitivity label

Use for detection method:

▼

Dictionary

File type

Keywords

Regular expression

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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".

NEW QUESTION 4

- (Topic 2)

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

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

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

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

Answer: B

Explanation:

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

From the provided table:

Device1 (Windows 11) - Supported Device2 (Windows 10) - Supported Device3 (iOS) - Not supported Device4 (macOS) - Not supported

Thus, only Device1 and Device2 support Endpoint DLP.

NEW QUESTION 5

- (Topic 2)

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.

NEW QUESTION 6

HOTSPOT - (Topic 2)

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:

To perform the action, assign the role of:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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.

NEW QUESTION 7

- (Topic 2)

Your company has offices in multiple countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management. You plan to perform the following actions:
 In a new country, open an office named Office1. Create a new user named User1.
 Deploy insider risk management to Office1.
 Add User1 to the Insider Risk Management Admins role group.
 You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.
 What should you create first?

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

Answer: C

Explanation:

To ensure User1 can perform insider risk management tasks only for the users and devices in Office1, the first step is to create an administrative unit in Microsoft Entra ID (formerly Azure AD). Administrative units allow you to scope permissions to specific users, devices, and locations. By creating an administrative unit for Office1 and assigning User1 to the Insider Risk Management Admins role group within that unit, User1 will only have access to users and devices in Office1.

NEW QUESTION 8

HOTSPOT - (Topic 2)

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

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

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

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

Answer Area

Statements

	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	<input type="checkbox"/>	<input type="checkbox"/>
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statement 1 - No. User1 is included in JIT protection. File1.docx is on Device1, which is onboarded to Microsoft Defender. However, File1.docx has not been evaluated for file classification, meaning JIT cannot enforce protection on it. If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.
 Statement 2 - No. User2 is not configured for JIT protection (JIT does not apply to them). File2.pdf has been evaluated for classification, but since User2 is not included in JIT protection, no blocking occurs. If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.

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

NEW QUESTION 9

- (Topic 2)

You have a Microsoft 365 E5 subscription.

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

DRAG DROP - (Topic 2)

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:

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

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

NOTE: Each correct selection is worth one point.

Reports	Answer Area	Report
DLP policy matches	Rules that are applied without triggering a policy alert:	<input type="text"/>
False positive and override	The top 10 files that have matched DLP policies:	<input type="text"/>
Incident reports	Alerts that are miscategorized:	<input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

NEW QUESTION 10

- (Topic 2)

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.

NEW QUESTION 12

- (Topic 2)

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

You configure an advanced DLP rule in the policy. Which type of condition can you use in the rule?

- A. Sensitive info type
- B. Content search query
- C. Sensitive label
- D. Keywords

Answer: A

Explanation:

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

NEW QUESTION 17

HOTSPOT - (Topic 2)

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:

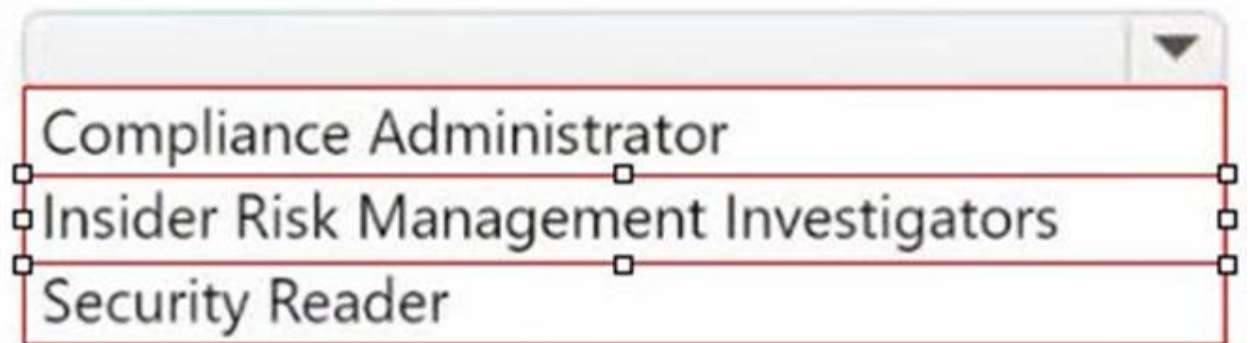
View recommendations from the Recommendations page. View the user risk level for all events by using Activity explorer. The solution must follow the principle of least privilege.

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

View the recommendations:



View the user risk level:



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 18

- (Topic 2)

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.

NEW QUESTION 20

- (Topic 2)

You have a Microsoft 365 subscription. Users have devices that run Windows 11.

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

Deletes files that contain a sensitive information type (SIT) from their device
 Copies files that contain a SIT to a USB drive
 Prints files that contain a SIT
 You need to prepare the environment to support the policy.
 What should you do?

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

Answer: D

Explanation:

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

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

NEW QUESTION 21

HOTSPOT - (Topic 2)

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

User1:

- 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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

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.

NEW QUESTION 26

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	Exchangeltem	MailboxLogin	None	90 Days
20	AuditRetention2	Exchangeltem	Send, MailltemsAccesssed	User1	9 Months
30	AuditRetention3	Sharepoint	None	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	None	10 Years

The users perform the following actions:

User1 renames a Microsoft SharePoint Online site. User2 sends an email message.

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

NOTE: Each correct selection is worth one point.

Answer Area

User1 renames a SharePoint site:

▼

- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

User2 sends an email message:

▼

- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 29

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1.

You plan to create the items shown in the following table.

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

Which items can use Trainable 1?

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

Answer: D

Explanation:

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

* 1. Retention Labels (Label2) Supported

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

* 2. Retention Label Policies (Policy1) Supported

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

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

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

NEW QUESTION 31

DRAG DROP - (Topic 2)

You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.

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

Actions	Answer Area
<div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;">Publish the trainable classifier.</div>	<div style="border: 1px solid red; height: 40px; margin-bottom: 5px;"></div>
<div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;">Retrain the trainable classifier.</div>	<div style="border: 1px solid red; height: 40px; margin-bottom: 5px;"></div>
<div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;">Create the trainable classifier.</div>	<div style="border: 1px solid red; height: 40px; margin-bottom: 5px;"></div>
<div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;">Test the trainable classifier.</div>	
<div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;">Create a terms of use (ToU) policy.</div>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

* 1. Create the trainable classifier

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

* 2. Test the trainable classifier

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

* 3. Publish the trainable classifier

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

NEW QUESTION 34

- (Topic 2)

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.

NEW QUESTION 39

- (Topic 2)

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

NEW QUESTION 44

- (Topic 2)

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.

NEW QUESTION 47

- (Topic 2)

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.

What should you do?

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

Answer: B

Explanation:

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

NEW QUESTION 52

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You plan to implement insider risk management for users that manage sensitive data associated with a project.

You need to create a protection policy for the users. The solution must meet the following requirements:

Minimize the impact on users who are NOT part of the project. Minimize administrative effort.

What should you do first?

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

Answer: B

Explanation:

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

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

NEW QUESTION 55

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SC-401 Practice Exam Features:

- * SC-401 Questions and Answers Updated Frequently
- * SC-401 Practice Questions Verified by Expert Senior Certified Staff
- * SC-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-401 Practice Test Here](#)