

Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365



NEW QUESTION 1

- (Topic 1)

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?
Admin1	Global Reader	<input type="checkbox"/> No, read-only permissions.
Admin2	Compliance Data Administrator	<input type="checkbox"/> Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	<input type="checkbox"/> Yes, has full compliance management, including labels.
Admin4	Security Operator	<input type="checkbox"/> No, this role is focused on security alerts and response.
Admin5	Security Administrator	<input type="checkbox"/> No, primarily focused on security policies and threat management.

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

NEW QUESTION 2

HOTSPOT - (Topic 2)

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

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Google Chrome:

▼

Config1 only

Config2 only

Config1 and Config2 only

Config2 and Config3 only

Config1, Config2, and Config3

Firefox:

▼

Config1 only

Config2 only

Config1 and Config2 only

Config2 and Config3 only

Config1, Config2, and Config3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft Purview browser extensions for Endpoint DLP are supported on: Windows 10/11 (Config1)
 macOS (Config2)
 Not supported on Android (Config3)
 Since Microsoft Purview does not support browser extensions on Android, Config3 is excluded from both Google Chrome and Firefox.

NEW QUESTION 3

HOTSPOT - (Topic 2)

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:

Admin1 and Admin2 only

Admin2 and Admin3 only

Admin3 and Admin4 only

Admin2, Admin3, and Admin4 only

Admin1, Admin2, Admin3, and Admin4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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:

Admin1 (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.

NEW QUESTION 4

- (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 5

- (Topic 2)

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 non-sensitive content.

NEW QUESTION 6

- (Topic 2)

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.

NEW QUESTION 7

- (Topic 2)

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.

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

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
<input type="checkbox"/> DLP policy matches	Rules that are applied without triggering a policy alert:	<input type="text"/>
<input type="checkbox"/> False positive and override	The top 10 files that have matched DLP policies:	<input type="text"/>
<input type="checkbox"/> 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 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 10

- (Topic 2)

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

Setting	Value
Location	<ul style="list-style-type: none"> • Exchange email (All recipients) • SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
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: AF

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.

NEW QUESTION 14

- (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 16

- (Topic 2)

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.

NEW QUESTION 18

- (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. You are creating an exact data match (EDM) classifier named EDM1.

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

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

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

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

Answer: B

Explanation:

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

From the provided table, the Match mode indicates how data is analyzed: PP (EU Passport Number) Likely a primary element because it's unique.

Name (All Full Names) Typically not a primary element as names are common.

DateOfBirth (Single-token) Usually a secondary element, not unique. AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier.

Since EDM supports a maximum of two primary elements, the correct answer is 2.

NEW QUESTION 23

HOTSPOT - (Topic 2)

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
- a Data loss prevention (DLP)
- 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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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.

NEW QUESTION 24

HOTSPOT - (Topic 2)

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

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

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

Name	Role
User1	Site owner
User2	Site member

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

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

User2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

User2:

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 30

- (Topic 2)

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.

NEW QUESTION 33

- (Topic 2)

You have Microsoft 365 E5 subscription.

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

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

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

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

Answer: D

Explanation:

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

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policy1	10:00:00	Yes
Policy2	10:00:03	Yes
Policy1	10:00:04	No (Duplicate within 5 min)
Policy2	10:00:31	No (Duplicate within 5 min)
Policy1	10:01:01	Yes
Policy1	10:04:45	Yes

Policy1 at 10:00:04 is ignored because Policy1 already triggered at 10:00:00, and it's within 5 minutes.

Policy2 at 10:00:31 is ignored because Policy2 already triggered at 10:00:03, and it's within 5 minutes.

Policy1 at 10:01:01 is a new alert because it's over 1 minute after the previous Policy1 alert.

Policy1 at 10:04:45 is a new alert because it's over 3 minutes after the previous Policy1 alert.

NEW QUESTION 38

- (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 42

- (Topic 2)

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.

NEW QUESTION 45

- (Topic 2)

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.

NEW QUESTION 48

- (Topic 2)

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: AE

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.

NEW QUESTION 49

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management. You implement the HR data connector.

You need to prepare the data that will be imported by the data connector. In which format should you prepare the data?

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

Answer: B

Explanation:

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

NEW QUESTION 54

- (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 56

.....

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](#)