



Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Topic 1)

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.

NEW QUESTION 2

- (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 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

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.

You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	None	Enabled

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

File	Label
File1	None
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



NEW QUESTION 6

HOTSPOT - (Topic 2)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 7

HOTSPOT - (Topic 2)

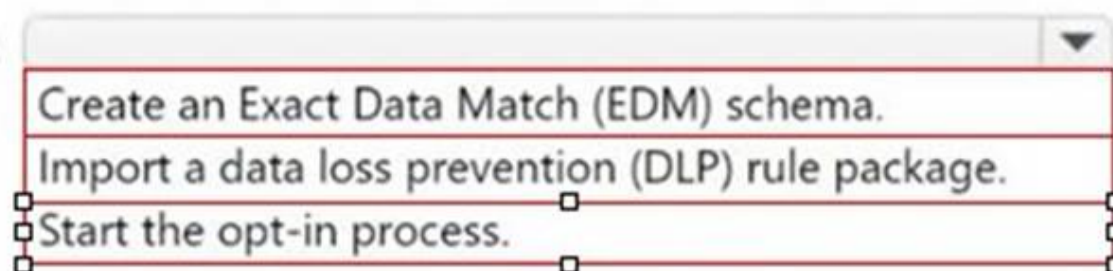
You have a new Microsoft 365 E5 tenant.

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 8

- (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 9

- (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 10

- (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-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.

NEW QUESTION 10

- (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 12

- (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 17

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 20

- (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 25

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:

Compliance Administrator
Insider Risk Management Investigators
Security Reader

View the user risk level:

Compliance Administrator
Insider Risk Management Analysts
Insider Risk Management Investigators
Security Reader

- 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 30

HOTSPOT - (Topic 2)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Since you are looking for a specific pattern (PA followed by eight digits, e.g., PA 12345678), the best classification method is Sensitive Info Type. Sensitive

Info Types allow pattern-based matching to identify structured data. Exact Data Match (EDM) is not needed because you're not comparing against a fixed dataset. Trainable classifier is not appropriate because this is a structured pattern, not an unstructured document classification. Box 2: Since PA 12345678 follows a structured pattern, the most effective method is Regular Expression (Regex). A Regular Expression (Regex) can be written to match "PA" followed by exactly eight digits (e.g., PA\s\d{8}). Keyword dictionary is not ideal because it works for predefined words, not number patterns. Function is unnecessary because there is no need for checksum validation or predefined validation rules.

NEW QUESTION 32

HOTSPOT - (Topic 2)

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

In Activity explorer:

A dropdown menu with a downward arrow on the right. Three options are visible and highlighted with red boxes: "Add a custom column", "Apply a built-in filter", and "Customize the default filter".

File type:

A dropdown menu with a downward arrow on the right. Four options are visible and highlighted with red boxes: "CSV", "JSON", "TXT", and "XML".

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 35

- (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 37

DRAG DROP - (Topic 2)

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.

Settings	Answer Area	Setting
Additional checks	Match product serial numbers that contain a 10-character alphanumeric string:	
Character proximity	Ensure that the abbreviation of SN appears within six characters of each product serial number:	
Confidence level	Exclude a test serial number of 1111111111 from a match:	
Primary element		
Supporting elements		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings	Answer Area	Setting
Additional checks	Match product serial numbers that contain a 10-character alphanumeric string:	Primary element
Character proximity	Ensure that the abbreviation of SN appears within six characters of each product serial number:	Character proximity
Confidence level	Exclude a test serial number of 1111111111 from a match:	Additional checks
Primary element		
Supporting elements		

NEW QUESTION 40

HOTSPOT - (Topic 2)

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

Create:

- A sensitive info type
- A trainable classifier
- An adaptive scope

Element:

- Functions
- Keyword dictionary
- Regular expression

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Create:

- A sensitive info type
- A trainable classifier
- An adaptive scope

Element:

- Functions
- Keyword dictionary
- Regular expression

NEW QUESTION 41

- (Topic 2)

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.

NEW QUESTION 45

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	Exchangelitem	MailboxLogin	None	90 Days
20	AuditRetention2	Exchangelitem	Send, MailItemsAccessed	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 Exchangelitem 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 47

- (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 51

- (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 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 non-sensitive content.

NEW QUESTION 55

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

- Publish the trainable classifier.
- Retrain the trainable classifier.
- Create the trainable classifier.
- Test the trainable classifier.
- Create a terms of use (ToU) policy.

Answer Area

- 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 60

- (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 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.

NEW QUESTION 65

HOTSPOT - (Topic 2)

You have a Microsoft 365 subscription.

You plan to deploy an audit log retention policy.


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

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

NOTE: Each correct selection is worth one point.

Answer Area

Search

 Learn about audit

Searches completed 0	Active searches 0	Active unfiltered searches 0
Date and time range (UTC) *	Activities - friendly names	Users
Start <input type="text" value="Aug"/> <input type="text" value="00:00"/>	<input type="text" value="Choose which activities to search ..."/>	<input type="text" value="Add the users whose audit logs you ..."/>
End <input type="text" value="Aug"/> <input type="text" value="00:00"/>	Activities - operation names	File, folder, or site
Keyword Search	<input type="text" value="Enter operation values, separated by ..."/>	<input type="text" value="Enter all or a part of the name of a fil..."/>
<input type="text" value="Enter the keyword to search for"/>	Record types	Workloads
Admin Units	<input type="text" value="Select the record types to search f..."/>	<input type="text" value="Enter the workloads to search for"/>
<input type="text" value="Choose which Admin Units to se..."/>	Search name	
	<input type="text" value="Give the search a name"/>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To validate whether an audit log retention policy will apply to the intended entries, you should configure the following fields:
 Date and time range (UTC) ensures that you are searching for audit logs within the time period when the policy should be applied. Audit logs are time-sensitive, and policies affect logs based on their timestamp.
 Record types allows you to filter and search for specific audit log categories (e.g., Exchange, SharePoint, Teams, etc.) that are affected by the retention policy. Selecting the correct record type ensures that the policy is evaluated against the relevant data.

NEW QUESTION 67

- (Topic 2)
 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.

NEW QUESTION 71

- (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 72

- (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 75

- (Topic 2)

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 Group1, 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.

NEW QUESTION 80

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

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

Sensitive info in email with subject 'Message1'

Details Sensitive info types Metadata

Event details

ID 173fe9ac-3a65-41b0-9914-1db451bba639 Location Exchange

Time of activity Jun 6, 2022 8:22 PM

Impacted entities

User Megan Bowen Email recipients victoria@fabrikam.com

Email subject Message1

Policy details

DLP policy matched Policy1 Rule matched Rule1

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 Document1.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 Rule1
was uninvolved in the override process

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 Rule1
was uninvolved in the override process

NEW QUESTION 83

- (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 84

- (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 87

- (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 89

.....

Relate Links

100% Pass Your SC-401 Exam with Exam Bible Prep Materials

<https://www.exambible.com/SC-401-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>