Free Questions for SC-400 by certscare

Shared by Gilmore on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Task 10

You plan to create a data loss prevention (DLP) policy that will apply to content containing the following keywords:

* Tailspin

* litware

* Falcon

You need to create a keyword list that can be used in the DLP policy. You do NOT need to create the DLP policy at this time.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To retain all Microsoft Exchange items in Alex Wilber's mailbox that contain the word ''Falcon'' and were created in the year 2021, follow these steps:

Create a Retention Policy:

Sign in to theMicrosoft 365 compliance center.

Navigate toPoliciesand click onRetention.

Create a new retention policy (e.g., ''Falcon Retention 2021'').

Specify the retention period (e.g.,2 yearsfrom the creation date).

Set the condition to include items containing the word ''Falcon.''

Apply the Retention Policy to Alex Wilber's Mailbox:

Assign the retention policy to Alex Wilber's mailbox.

Ensure that the policy targets items created in the year 2021.

Validate the Policy:

Test the policy thoroughly to ensure it correctly retains the specified items.

Monitor the mailbox to verify that the retention actions are enforced.

Question 2

Question Type: MultipleChoice

Task 9

You are investigating a data breach.

You need to retain all Microsoft Exchange items in the mailbox of Alex Wilber that contain the word Falcon and were created in the year 2021.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To retain all Microsoft Exchange items in Alex Wilber's mailbox that contain the word "Falcon" and were created in the year 2021, follow these steps:

Create a Retention Policy:

Sign in to theMicrosoft 365 compliance center.

Navigate toPoliciesand click onRetention.

Create a new retention policy (e.g., "Falcon Retention 2021").

Specify the retention period (e.g.,2 yearsfrom the creation date).

Set the condition to include items containing the word "Falcon."

Apply the Retention Policy to Alex Wilber's Mailbox:

Assign the retention policy to Alex Wilber's mailbox.

Ensure that the policy targets items created in the year 2021.

Validate the Policy:

Test the policy thoroughly to ensure it correctly retains the specified items.

Monitor the mailbox to verify that the retention actions are enforced.

Question 3

Question Type: **MultipleChoice**

Task 8

You need to retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created, and then delete them.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To set up a retention policy for Microsoft SharePoint files containing the word ''Falcon,'' follow these steps:

Create a Retention Label:

Retention labels allow you to specify retention periods for content. Go to your SharePoint site or library where you want to apply the policy.

Open the document library settings.

Under "Permissions and Management," select "Apply label to items in this list or library."

Choose the retention label that corresponds to the desired retention period (e.g., "Falcon Retention - 2 years").

Configure the Retention Label:

Specify the retention period (in this case,2 years).

Define the action to be taken after the retention period (e.g., move to recycle bin).

Apply the Retention Label:

Tag the relevant content (files containing the word "Falcon") with the retention label.

The policy will automatically retain the files for two years from their creation date and then delete them.

Question 4

Question Type: MultipleChoice

Task 7

You need to create a retention policy that meets the following requirements:

* Applies to Microsoft Teams chat and Teams channel messages of users that have a department attribute of Sales.

* Retains item for five years from the date they are created, and then deletes them.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To create a retention policy for Microsoft Teams that meets the specified requirements, follow these steps:

Sign in to the Microsoft 365 compliance center:

Log in to the Office 365 Admin Portal.

Visit the Microsoft 365 compliance center.

Navigate to Retention Policies:

SelectPolicies, then click onRetention.

Create a New Retention Policy:

Click onNew retention policy.

Provide aNamefor your new retention policy (e.g., "Sales Teams Retention Policy").

Optionally, add aDescription.

Select the Location:

Choose the location to which the policy will be applied. In this case, selectMicrosoft Teams.

Configure Retention Settings:

Set the retention period to5 yearsfrom the date items are created.

Specify whether you want to retain or delete the content after the retention period.

Apply the Policy:

Save your changes.

This policy will now apply to Microsoft Teams chat and channel messages for users with a department attribute of "Sales," retaining items for five years before automatic deletion

Question 5

Question Type: **MultipleChoice**

Task 6

You plan to implement Endpoint data loss prevention (Endpoint DLP) policies for computers that run Windows.

Users have an application named App1 that stores data locally in a folder named C:\app1\data.

You need to prevent the folder from being monitored by Endpoint DLP.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To prevent the folderC:\app1\datafrom being monitored byEndpoint Data Loss Prevention (DLP), follow these steps:

Configure File Path Exclusions:

Open theMicrosoft Purview compliance portal.

Navigate toData loss prevention>Overview>Data loss prevention settings>Endpoint settings.

Look for theFile path exclusionssection.

Add an exclusion for the pathC:\app1\data.

Files within this folder will not be audited or subject to DLP policy enforcement12.

Remember to validate this configuration and ensure that the folder is excluded from DLP monitoring

Question 6

Question Type: MultipleChoice

Task 5

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

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To allow theU.S. Salesgroup to store files containing information subject to theGeneral Data Protection Regulation (GDPR)in their OneDrive accounts while keeping other GDPR restrictions intact, follow these steps:

Create a Security Group:

Log in to theMicrosoft 365 admin center.

Navigate toGroupsand create a new security group called"U.S. Sales".

Configure OneDrive Sharing Settings:

Go to theSettings > Org settingspage.

On theServicestab, selectMicrosoft 365 on the web.

Choose whether to let users open files stored in third-party storage services in Microsoft 365 on the web.Ensure this setting aligns with your organization's GDPR requirements1.

Set Specific Sharing Permissions:

Set the default OneDrive share type to"Specific People"under theSharingmenu in the OneDrive admin area.

Right-click the folder inOneDrive online, clickShare.

Click themore button (three dots)in theSend Linkheader.

ClickManage Access.

ClickGrant Access, then add the"U.S. Sales"security group.This access will apply only to that group2.

By following these steps, theU.S. Salesgroup will be able to store GDPR-related files in their OneDrive accounts while maintaining compliance with other GDPR restrictions

Question 7

Question Type: **MultipleChoice**

Task 4

You need to block users from sending emails containing information that is subject to Payment Card Industry Data Security Standard (PCI OSS). The solution must affect only emails.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To block users from sending emails containing information subject to thePayment Card Industry Data Security Standard (PCI DSS), you can create aData Loss Prevention (DLP) policyinMicrosoft Exchange Online. Here's how:

Create a Custom DLP Policy:

Log in to theMicrosoft Exchange Online admin center.

Navigate toData loss prevention>Policy.

Create a new custom policy specifically for PCI DSS compliance.

Define Conditions:

In the policy settings, define conditions that identify sensitive data related to PCI DSS. For example:

Keywords: Include terms like "credit card," "debit card," or specific card number formats.

Regular Expressions (Regex): Craft expressions to match credit card patterns (e.g.,\b\d{4}-\d{4}-\d{4}-\d{4}\bfor Visa/Mastercard).

Sensitive Information Types: Use built-in or custom sensitive information types related to payment cards.

Choose Actions:

Specify the actions to take when sensitive data is detected in emails:

Block: Prevent the email from being sent.

Notify Sender: Inform the sender that sensitive data is not allowed via email.

Add Disclaimer/Watermark: Optionally add a disclaimer or watermark to the email.

Apply the Policy to Emails Only:

Ensure that the policy is configured to apply only toemails(not other communication channels).

Exclude internal communication if necessary.

Test and Monitor:

Enable the policy intest modeinitially to validate its effectiveness.

Monitor logs and adjust the policy as needed.

Question 8

Question Type: **MultipleChoice**

Task 3

You plan to automatically apply a watermark to the document1 of a project named Falcon.

You need to create a label that will add a watermark of 'Project falcon' in red. size-12 font diagonally across the documents.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To create a label that adds a watermark of "Project Falcon" in red, size-12 font diagonally across the documents, follow these steps:

Create a Sensitivity Label:

Log in to theMicrosoft Purview portalor theMicrosoft Purview compliance portalas an admin.

Navigate toSensitivity labelsand create a new label called"Project Falcon".

Specify the appropriate settings for this label, including encryption, content markings, and permissions.

Configure Content Markings (Watermark):

When creating the label, configure the content markings section.

Choose"Watermark"and set the text to"Project Falcon".

Select the color asredand font size as12.

Set the watermark position todiagonalacross the document.

Assign the Label:

Assign the"Project Falcon"label to the relevant documents within theFalcon project.

Users who apply this label will automatically add the specified watermark to their documents.

Question 9

Question Type: MultipleChoice

Task 2

You discover that all users can apply the Confidential - Finance label.

You need to ensure that the Confidential - Finance label is available only to the members of the Finance Team group.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

To restrict theConfidential - Financelabel to only the members of theFinance Teamgroup, follow these steps:

Create a Sensitivity Label:

Log in to theMicrosoft Purview portalor theMicrosoft Purview compliance portalas an admin.

Navigate toSensitivity labelsand create a new label called"Confidential - Finance".

Specify the appropriate settings for this label, including encryption, content markings, and permissions1.

Configure Encryption Settings:

When creating the label, ensure that you configure the encryption settings.

Choose either to assign permissions now (where you determine exactly which users get which permissions) or allow users to assign permissions when they apply the label to content2.

Assign the Label to the Finance Team Group:

In theMicrosoft Purview portal, go to theGroupssection.

Select theFinance Teamgroup.

UnderSettings, chooseSensitivity labels.

Add the"Confidential - Finance"label to this group.

Only members of theFinance Teamwill now have access to this label3.

Test the Configuration:

Question 10

Question Type: **MultipleChoice**

Task 1

You need to provide users with the ability to manually classify files that contain product information that are stored in SharePoint Online sites. The solution must meet the following requirements:

* The users must be able to apply a classification of Product1 to the files.

* Any authenticated user must be able to open files classified as Product1.

* files classified as Product1 must be encrypted.

Options:

A) See the solution below in Explanation

Answer:

A

Explanation:

Create a Custom Content Type:

Go to your SharePoint Online site.

Click onSettings(gear icon) and selectSite settings.

UnderWeb Designer Galleries, chooseSite content types.

Create a new content type (e.g., "Product1 Classification") based on theDocumentparent content type.

Add a custom column (e.g., "Classification") to this content type.

Apply the Content Type to Document Libraries:

Navigate to the document library where the files are stored.

Click onLibrary settings.

UnderGeneral Settings, selectAdvanced settings.

ChooseYesfor "Allow management of content types."

Add your custom content type ("Product1 Classification") to the library.

Manually Classify Files:

Upload or edit a file in the library.

In the file properties, select theClassificationfield and set it to "Product1."

Permissions and Encryption:

Ensure that all authenticated users have at leastViewpermissions on the library.

For encryption, SharePoint Online automatically encrypts files at rest usingBitLockerdisk-level encryption.

Files classified as "Product1" will be encrypted and accessible only to authorized users.