

Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365



NEW QUESTION 1

DRAG DROP - (Topic 1)

You need to meet the technical requirements for the Site1 documents.

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Step 1: Create a Sensitive Info Type

A sensitive info type is needed to detect credit card numbers in documents.

Microsoft Purview includes built-in sensitive info types for credit card numbers, but we can also create a custom one if necessary.

Step 2: Create a Sensitivity Label

A sensitivity label is required to classify and protect documents containing sensitive information.

This label can apply encryption, watermarking, or access controls to credit card data.

Step 3: Create an Auto-Labeling Policy

An auto-labeling policy ensures that the sensitivity label is applied automatically when credit card numbers are detected in Site1.

This policy is configured to scan files and automatically apply the correct sensitivity label.

NEW QUESTION 2

- (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 3

- (Topic 2)

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.

You need to implement a data loss prevention (DLP) solution that meets the following requirements:

- Email messages that contain a single customer identifier can be sent outside your company.
- Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a sensitivity label
- B. a sensitive information type
- C. a DLP policy
- D. a retention label
- E. a mail flow rule

Answer: BC

Explanation:

You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.

A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

NEW QUESTION 4

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 5
 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 6

- (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 7

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 8

- (Topic 2)

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

Name	Description
User1	- User 1 is a regional manager. - User1 is assigned the Reader role. - Three department managers report to User1.
User2	- User2 is the human resources (HR) department manager. - User2 has no Microsoft Entra roles assigned. - Five HR department users report to User2.
User3	- User3 is a developer. - User3 reports to User2. - User3 is the only user in the compliance department. - User3 is assigned the Compliance Administrator role.
User4	- User4 is the assistant of User1. - User4 has no Microsoft Entra roles assigned. - User4 handles a high volume of confidential data on behalf of User1.

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

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

Answer: D

Explanation:

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

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

Holds a managerial position (regional manager).

Manages multiple department managers, indicating organizational influence. Access to critical business information.

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

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

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

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

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

Risk Factors:

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

Potentially high impact on compliance and security settings.

Flagged? -Yes (Privileged Compliance Administrator role).

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

Risk Factors:

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

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

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

NEW QUESTION 9

- (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 10

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

If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.

Yes

No

If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.

Yes

No

If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.

Yes

No

- 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 10

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:

- A group mailbox
- Microsoft Teams channel messages
- A Microsoft SharePoint Online teams site

You create the objects shown in the following table.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Name	Type	Description
RLabel1	Retention label	<i>None</i>
AutoApply1	Auto-labeling policy	Applies RLabel1 to Group1
Retention1	Retention policy	Applied to Group2

To which resources will AutoApply1 and Retention1 be applied? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

AutoApply1:

The group mailbox only

The SharePoint Online teams site only

The group mailbox and SharePoint Online teams site only

The group mailbox and Teams channel messages only

The group mailbox, SharePoint Online teams site, and Teams channel messages

Retention1:

The group mailbox only

The SharePoint Online teams site only

The group mailbox and SharePoint Online teams site only

The group mailbox and Teams channel messages only

The group mailbox, SharePoint Online teams site, and Teams channel messages

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 AutoApply1 is an auto-labeling policy that applies RLabel1 to Group1. Auto-labeling policies can apply retention labels across group mailboxes, SharePoint Online sites, and Teams channel messages if they are configured for group resources.
 Retention1 is a retention policy applied to Group2. Retention policies for Microsoft 365 groups apply to all group resources, including group mailboxes, SharePoint Online teams sites, and Teams channel messages.
 Since both AutoApply1 and Retention1 affect entire groups, they apply to all associated resources: group mailbox, SharePoint Online teams site, and Teams channel messages.

NEW QUESTION 15

- (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	- 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 20

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:

	▼
☐	Add a custom column
☐	Apply a built-in filter
☐	Customize the default filter

File type:

	▼
☐	CSV
☐	JSON
☐	TXT
☐	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 24

- (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 29

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 34

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents.

You plan to implement Microsoft 365 Copilot for the subscription.
You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.
What should you use?

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

Answer: D

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

NEW QUESTION 36

- (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 39

HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

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

The subscription contains the users shown in the following table.

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

You need to review the activities.
What should you use for each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User1:

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

Audit log search

Insider risk audit log

Unified Catalog

User2:

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

Audit log search

Insider risk audit log

Unified Catalog

User3:

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

Audit log search

Insider risk audit log

Unified Catalog

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.
User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI- related activity cannot be tracked in DSPM for AI. Instead, Audit log search should be used to review activity such as using Microsoft 365 Copilot.
User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

NEW QUESTION 42
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, MaillItemsAccesssed	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 ExchangeItem is covered under the AuditRetention2 policy, but this policy applies only to User1. Since User2 is not covered under a specific policy, the default retention period for audit logs in Microsoft Purview is 90 days.

NEW QUESTION 43

- (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 46

DRAG DROP - (Topic 2)
You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
0 Publish the trainable classifier.	0
0 Retrain the trainable classifier.	0
0 Create the trainable classifier.	0
0 Test the trainable classifier.	
0 Create a terms of use (ToU) policy.	

- 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 51

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) *

Start

Aug

00:00

End

Aug

00:00

Activities - friendly names

Choose which activities to search ...

Activities - operation names ⓘ

Enter operation values, separated by ...

Record types

Select the record types to search f...

Search name

Give the search a name

Keyword Search

Enter the keyword to search for

Admin Units

Chonse which Admin Units to se...

Users

Add the users whose audit logs you ...

File, folder, or site ⓘ

Enter all or a part of the name of a fil...

Workloads

Enter the workloads to search for

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

- 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 52

- (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 57

- (Topic 2)

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

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

You need to identify and categorize the resumes. The solution must minimize administrative effort.

What should you include in the solution?

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

Answer: A

Explanation:

Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice.

Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.

Final Approach:

Train a trainable classifier using sample resumes. Deploy the classifier in Microsoft Purview.

Configure a sensitivity label to be automatically applied when a document matches the classifier.

NEW QUESTION 62

- (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 67

- (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 71

- (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 a sensitive info type. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

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

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

NEW QUESTION 75

- (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 78

- (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 83

- (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 Defender for Cloud Apps, you mark the application as Unsanctioned.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Marking Tailspin_scanner.exe as "Unsanctioned" in Microsoft Defender for Cloud Apps only blocks its usage in cloud-based activities (such as accessing SharePoint, OneDrive, or Exchange Online). However, it does not prevent a locally installed application on Windows 11 devices from accessing sensitive files.

To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list. Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

NEW QUESTION 86

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1. You plan to enable co-authoring for encrypted files.

You need to ensure that files that have label1 applied support co-authoring.

Which two settings should you modify? To answer, select the settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- ☐ Remove access control settings if already applied to items
- ☒ Configure access control settings

 Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires 

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access 

Always

Assign permissions to specific users and groups * 

[Assign permissions](#)

0 items

Users and groups

Permissions

Edit

Delete

No data available

☒ Use dynamic watermarking 

 Customize text (optional)

☒ Use Double Key Encryption 

<https://sts.contoso.com>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

NEW QUESTION 90

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

|



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 94

- (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 97

- (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 99

HOTSPOT - (Topic 2)

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

Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label1.
 You need to publish Label1 and have the label apply automatically.
 To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

Publish to:

▼

Site1 only

Group1 only

Group1 and Group2 only

Group1 and Site1 only

Site1 and Team1 only

Group1, Group2, Site1, and Team1

Auto-apply to:

▼

Site1 only

Group1 only

Group1 and Group2 only

Group1 and Site1 only

Site1 and Team1 only

Group1, Group2, Site1, and Team1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Publishing a Sensitivity Label

Sensitivity labels can be published to Microsoft 365 groups, security groups, SharePoint

Online sites, and Microsoft Teams. Since we have: Group1 (Microsoft 365 group) - Supported Group2 (Security group) - Supported

Site1 (SharePoint Online site) - Supported Team1 (Microsoft Teams team) - Supported

This means we can publish Label1 to Group1, Group2, Site1, and Team1. Box 2: Auto-Applying a Sensitivity Label

Auto-apply policies for sensitivity labels work on: SharePoint Online sites (documents)

OneDrive (documents) Exchange email (messages)

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

NEW QUESTION 104

.....

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 First Try
- * SC-401 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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