Vendor: Microsoft

Exam Code: SC-401

Exam Name: Administering Information Security in Microsoft 365

Version: DEMO

QUESTION 1
Case Study 1 - Contoso, Ltd

Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment
Microsoft 365 Environment
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

```
- Name: Site4RetentionPolicy1
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

- Name: Site4RetentionPolicy2
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing
```

Problem Statements
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements
Planned Changes
Contoso plans to create the following data loss prevention (DLP) policy:

```
- Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

- Instance count: 2 to any
Actions: Restrict access to the content
```

Technical Requirements
Contoso must meet the following technical requirements:

```
- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least
one year.
- Confidential documents must be detected and protected by using
Microsoft 365.
- Site1 documents that include credit card numbers must be labeled
automatically.
- All administrative users must be able to create Microsoft 365
sensitivity labels.
- After a project is complete, the documents in Site3 that relate to
the project must be retained for 10 years.
```

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: E
Explanation:
Admin3 (Compliance Administrator) already has this permission through their existing role.
The users who need the "Sensitivity Label Administrator" role assigned are those who do not already have the permission via another role. These are Admin1, Admin2, Admin4, and Admin5.

QUESTION 2
Case Study 1 - Contoso, Ltd

Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment
Microsoft 365 Environment
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

```
- Name: Site4RetentionPolicy1
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

- Name: Site4RetentionPolicy2
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing
```

Problem Statements
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements
Planned Changes
Contoso plans to create the following data loss prevention (DLP) policy:

```
- Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

- Instance count: 2 to any
Actions: Restrict access to the content
```

Technical Requirements
Contoso must meet the following technical requirements:

```
- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
```

- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

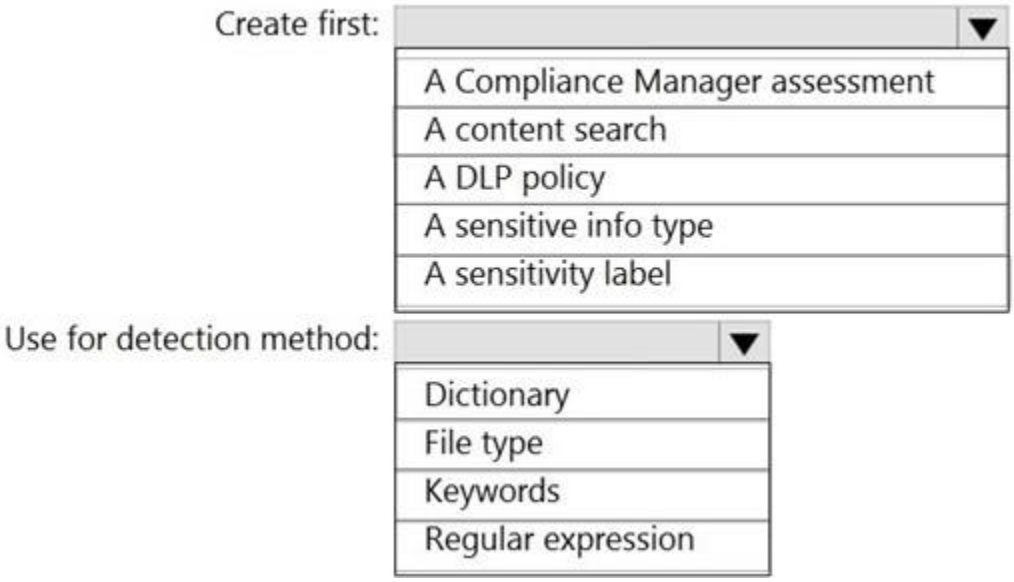
Hotspot Question

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.

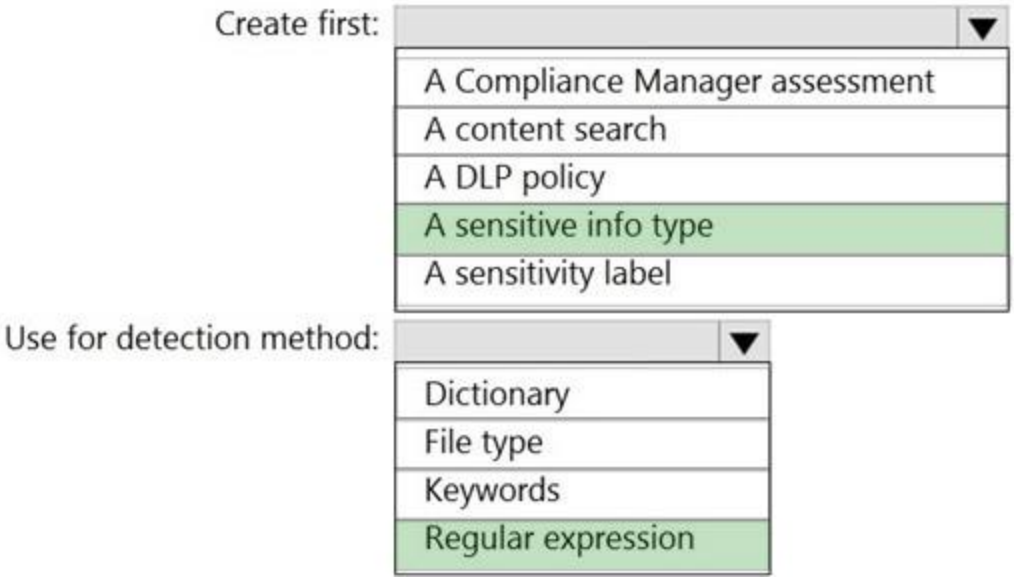
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:
Sensitive information types :
Identifies sensitive data by using built-in or custom regular expressions or a function.
Corroborative evidence includes keywords, confidence levels, and proximity.
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

QUESTION 3
You have a Microsoft 365 E5 subscription.

You need to enable support for sensitivity labels in Microsoft SharePoint Online.

What should you use?

A. the Microsoft Purview portal
B. the Microsoft Entra admin center
C. the SharePoint admin center
D. the Microsoft 365 admin center

Answer: C
Explanation:
To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center Settings Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

QUESTION 4
You have a Microsoft 365 subscription.

You need to customize encrypted email for the subscription. The solution must meet the following

requirements.

- Ensure that when an encrypted email is sent, the email includes the company logo.
- Minimize administrative effort.

Which PowerShell cmdlet should you run?

A. Set-IRMConfiguration
B. Set-OMEConfiguration
C. Set-RMSTemplate
D. New-OMEConfiguration

Answer: B
Explanation:
To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set-OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as:
- Company logo
- Custom text
- Background color
This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

QUESTION 5
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

QUESTION 6
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.

QUESTION 7
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:
With 1 policy you cannot choose both Audit and Block.
You need 1 policy for all users with block rule, and exclude group1 and 1 policy that includes group1 only and the rule set to Audit only.

QUESTION 8

You have a Microsoft 365 subscription.

You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Microsoft Defender for Cloud Apps, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint ad min center, modify the records management settings.
D. From the Microsoft Purview portal, publish a label.
E. From the Microsoft Purview portal, create a label.

Answer: DE
Explanation:
To allow users to apply retention labels to individual documents in Microsoft SharePoint libraries, you need to create a retention label and publish the label.
In Microsoft Purview, retention labels define how long content should be retained or deleted. You must first create a label that specifies the retention rules. After creating the label, you must publish it so that it becomes available for users in SharePoint document libraries. Once published, users can manually apply the retention label to individual documents.

QUESTION 9
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management.

What should you create first?

A. a sensitivity label policy
B. a data loss prevention (DLP) policy
C. an auto-labeling policy
D. a retention label

Answer: D
Explanation:
To implement Microsoft Purview Data Lifecycle Management for SharePoint Online (Site1), you need to create a retention label first. Retention labels define how long content should be retained or deleted based on compliance requirements. Once a retention label is created, it can be manually or automatically applied to content in SharePoint Online, Exchange, OneDrive, and Teams. After creating a retention label, you can configure label policies to apply them to Site1 and other locations.

QUESTION 10
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: B
Explanation:
If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Yammer locations.
https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention#create-and-configure-a-retention-policy

QUESTION 11
Hotspot Question

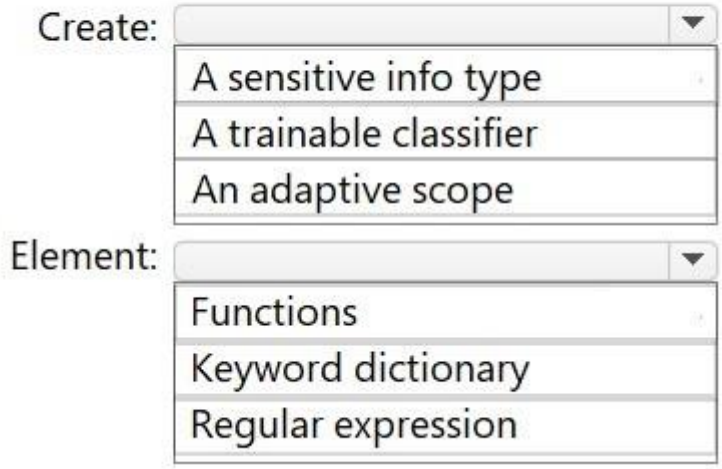
You have a Microsoft 365 E5 subscription.

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.

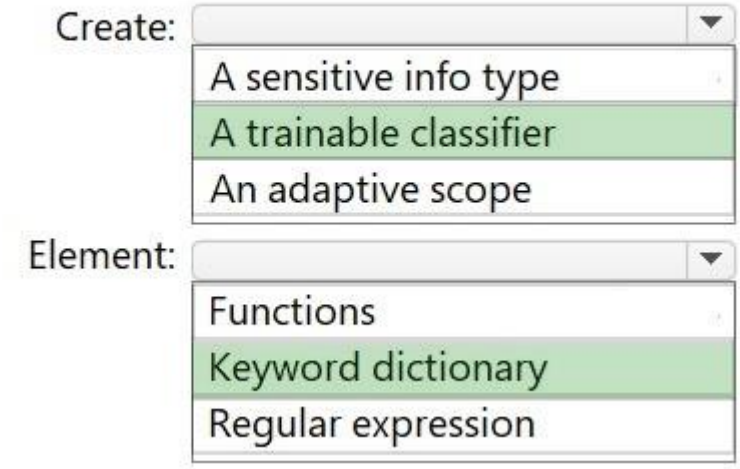
What should you create in the Microsoft Purview portal, and which type of element should you select? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:
To classify documents in SharePoint Online using Customer.csv, you need to create a trainable classifier. A trainable classifier is best suited for identifying patterns in unstructured data (e.g., customer names in documents). A sensitive info type is more suitable for structured data (e.g., credit card numbers, SSNs). An adaptive scope is used to apply policies dynamically based on attributes, not for classifying content.

Since Customer.csv contains a list of names, the best element to use is a keyword dictionary. A keyword dictionary allows you to upload a list of predefined terms (such as customer names) to classify documents based on their presence. Regular expressions are used for pattern-based detection (e.g., credit card numbers, serial numbers), which is not needed here. Functions are used for predefined sensitive data detection (e.g., checksum validation for credit card numbers), which does not apply in this case.

QUESTION 12
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.

QUESTION 13
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. 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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**