MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You plan to create a script to automate user mailbox searches. The script will search the mailbox of a user named Allan Deyoung for messages that contain the word injunction.

You need to create the search that will be included in the script.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See explanation below.

Step 1: Create a CSV file that contains information about the searches you want to run

The comma separated value (CSV) file that you create in this step contains a row for each user that want to search. You can search the user\\'s Exchange Online mailbox (which includes the archive mailbox, if it\\'s enabled) and their OneDrive for Business site. Or you can search just the mailbox or the OneDrive for Business site. You can also search any site in your SharePoint Online organization. The script that you run in Step 3 will create a separate search for each row in the CSV file.

1. Copy and paste the following text into a .txt file using NotePad. Save this file to a folder on your local computer. You\\'ll save the other scripts to this folder as well.

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2000,12/31/2005 sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2006,12/31/2010 sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2011,3/21/2016 ,https://contoso.sharepoint.com/sites/contoso,,,3/21/2016 ,https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com,,1/1/2015, ,https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com,,1/1/2015,

The first row, or header row, of the file lists the parameters that will be used by New-ComplianceSearch cmdlet to create a new Content Searches. Each parameter name is separated by a comma. Make sure there aren\\'t any spaces in the header row. Each row under the header row represents the parameter values for each search. Be sure to replace the placeholder data in the CSV file with your actual data.

2.

Open the .txt file in Excel, and then use the information in the following table to edit the file with information for each search.

3.

Save the Excel file as a CSV file to a folder on your local computer. The script that you create in Step 3 will use the information in this CSV file to create the searches.

Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search.
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-searches?view=o365-worldwide

Keyword queries and search conditions for Content Search https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365-worldwide

QUESTION 2

You need to ensure that when users tag documents as classified, a classified watermark is applied to the documents.

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See explanation below.

1.

In the admin center, select the Compliance admin center.

2.

Select Classification > Sensitivity labels.

3.

Select Create a label, and when the warning appears, select Yes.

4.

Enter a Label name, Tooltip, and Description. Select Next.

5.

Turn on Encryption. Choose when you want to assign permissions, whether you want your users\\' access to the content to expire, and whether you want to allow offline access.

6.

Select Assign permissions > Add these email addresses or domains.

7.

Enter an email address or domain name (such as Contoso.org). Select Add, and repeat for each email address or domain you want to add.

8.

Select Choose permissions from preset or custom.

9.

Use the drop-down list to select preset permissions, such as Reviewer or Viewer, or select Custom permissions. If you chose Custom, select the permissions from the list. Select Save >Save > Next.

10.

Turn on Content marking, and choose the markings you want to use.

11.

For each marking that you choose, select Customize text. Enter the text you want to appear on the document, and set the font and layout options. Select Save, and then repeat for any additional markings. Select Next.

12.

Optionally, turn on Endpoint data loss prevention. Select Next.

13.

Optionally, turn on Auto labeling. Add a condition. For example, under Detect content that contains, select Add a condition. Enter the condition; for example, add a condition that if passport, Social Security, or other sensitive information is detected, the label will be added. Select Next.

14.

Review your settings, and select Create. Your label has been created. Repeat this process for any additional labels you want.

15.

By default, labels appear in Office apps in this order: Confidential, Internal, and Public. To change the order, for each label, select More actions (the ellipsis), and then move the label up or down. Typically, permissions are listed from the lowest to highest level of permissions.

16.

To add a sub-label to a label, select More actions, then Add sub level.

17.

When finished, choose Publish labels> Choose labels to publish > Add. Select the labels you want to publish, and then select Add > Done > Next.

18.

By default, the new label policy is applied to everyone. If you want to limit who the policy is applied to, select Choose users or groups > Add. Select who you want the policy to apply to, and then select Add > Done > Next.

19.

If you want a default label for documents and email, select the label you want from the drop-down list. Review the remaining settings, adjust as needed, and then select Next.

20.

Enter a Name and Description for your policy. Select Next.

21.

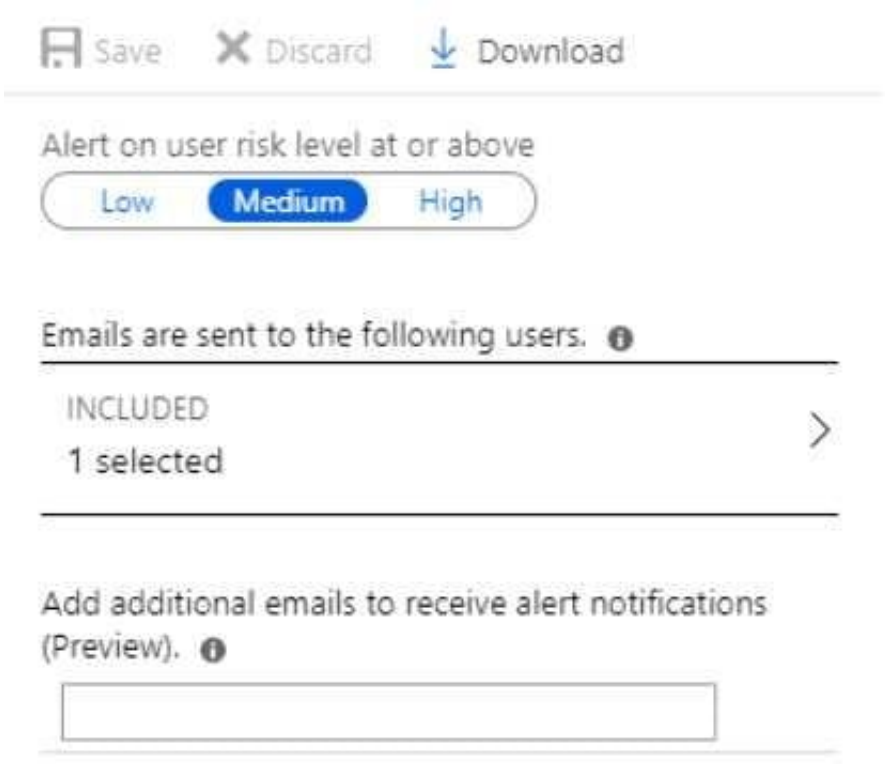
Review your settings, then select Publish.

Reference: https://support.office.com/en-us/article/create-and-manage-sensitivity-labels-2fb96b54-7dd2-4f0c-ac8d-170790d4b8b9 https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

QUESTION 3

HOTSPOT

You have a Microsoft 365 E5 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. Azure AD Identity Protection alerts for contoso.com are configured as shown in the following exhibit.



A user named User1 is configured to receive alerts from Azure AD Identity Protection. You create users in contoso.com as shown in the following table.

Name	Role
User2	Security reader
User3	User administrator
User4	*None*
User5	*None*

The users perform the sign-ins shown in the following table.

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	○	○
User2 receives three email alerts from Azure AD Identity Protection.	○	○
User3 receives two email alerts from Azure AD Identity Protection.	○	○

Correct Answer:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	○	○
User2 receives three email alerts from Azure AD Identity Protection.	○	○
User3 receives two email alerts from Azure AD Identity Protection.	○	○

Box 1: No

User1 will receive the two alerts classified as medium or higher. Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some

are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as Low.

Box 2: No

User2 will receive the two alerts classified as medium or higher. Email alerts are sent to all global admins, security admins and security readers Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not

user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as Low.

Box 3: No

User3 will not receive alters.

Email alerts are sent to all global admins, security admins and security readers.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

QUESTION 4

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Cloud Apps enabled. You need to create an alert in Defender for Cloud Apps when source code is shared externally.

Which type of policy should you create?

A. Cloud Discovery anomaly detection

B. file

C. access

D. activity

Correct Answer: B

Detect externally shared source code

Detect when files that contain content that might be source code are shared publicly or are shared with users outside of your organization.

Prerequisites

You must have at least one app connected using app connectors.

Steps

1.

On the Policies page, create a new File policy.

2.

Select and apply the policy template Externally shared source code

3.

Optional: Customize the list of file Extensions to match your organization\\'s source code file extensions.

4.

Optional: Set the Governance actions to be taken on files when a violation is detected. The governance actions available vary between services. For example, in Box, Send policy-match digest to file owner and Put in admin quarantine.

5.

Select and apply the policy template Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/policies-information-protection#detect-externally-shared-source-code

QUESTION 5

Your company has a Microsoft 365 E5 subscription that contains a user named User.

User1 leaves the company.

You need to identify all the personal data of User1 that is stored in the subscription.

What should you do in the Microsoft Purview compliance portal?

A. Create an eDscovery case.

B. Perform an audit.

C. Perform a content search.

D. Submit a Data Subject Request (DSR).

Correct Answer: D

Find and export a user\\'s personal data to help you respond to data subject requests for the General Data Protection Regulation (GDPR). https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365- worldwide