



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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

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 the Cloud App Security admin center, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the SharePoint admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security admin center, publish a label.

Correct Answer: CE

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp>

QUESTION 2

You need to ensure that a user named Allan Deyoung can perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. The solution must use the principle of least privilege.

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

Correct Answer: See explanation below.

1.

After signing in to the Microsoft 365 admin center, navigate to the Security and Compliance Center.

2.

In the left pane of the security and compliance center, select Permissions, and then select the checkbox next to eDiscovery Manager.

3.

On the eDiscovery Manager flyout page, do one of the following based on the eDiscovery permissions that you want to assign.

To make a user an eDiscovery Manager: Next to eDiscovery Manager, select Edit. In the Choose eDiscovery Manager section, select the Choose eDiscovery Manager hyperlink, and then select + Add. Select the user (or users) you

want to add as an eDiscovery manager, and then select Add. When you're finished adding users, select Done. Then, on the Editing Choose eDiscovery Manager flyout page, select Save to save the changes to the eDiscovery Manager



membership.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide>

QUESTION 3

You have a Microsoft 365 subscription and a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) subscription. You have devices enrolled in Microsoft Endpoint Manager as shown in the following table:

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You integrate Microsoft Defender ATP and Endpoint Manager. You plan to evaluate the Microsoft Defender ATP risk level for the devices. You need to identify which devices can be evaluated. Which devices should you identify?

- A. Device1 and Device2 only
- B. Device1 only
- C. Device1 and Device3 only
- D. Device2 and Device3 only

Correct Answer: B

Microsoft Defender ATP supports Windows 10, Windows Server, macOSX, and Linux

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/evaluation-lab>
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/minimumrequirements>

QUESTION 4

HOTSPOT

You have a Microsoft 365 E5 subscription.

Users and device objects are added and removed daily. Users in the sales department frequently change their device.

You need to create three following groups:



Group	Requirement
1	All the devices of users where the Department attributes is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

The solution must minimize administrative effort.

What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

Correct Answer:



Answer Area

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

Group 1 has to be assigned because you can't create a device group based on the device owners' attributes.

Group 2 can be dynamic because a user does have a department attribute.

Group 3 can be dynamic because a device does have a deviceownership attribute.

QUESTION 5

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the data loss prevention (DLP) policies in following table.

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown in the following table.



Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

All the policies are assigned to Site1.

You need to ensure that if a user uploads a document to Site1 that matches all the rules, the user will be shown the Tip 2 policy tip.

What should you do?

- A. Enable additional processing Of the policies if is a match for Rule1.
- B. Change the priority Of DLP2 to 3.
- C. Change the priority of DLP2 to 0
- D. Prevent additional processing of the policies if there is a match for Rule2.

Correct Answer: C

The rule with priority 0 is processed first.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference>

QUESTION 6

You plan to deploy a new Microsoft 365 Subscription that will contain 500 users.

You need to ensure that the following actions are performed the users sign in to the subscription

Evaluate the users\' risk level based on their location and travel. Require high-risk users to sign in by using Azure Multi-Factor Authentication (Azure MFA).

The solution must minimize cost.

Which license should you assign to each user?

- A. Microsoft 365 Business Premium
- B. Microsoft 365 E3
- C. Enterprise Mobility + Security E3
- D. Microsoft 365 ES

Correct Answer: A



QUESTION 7

You need to ensure that email messages in Exchange Online and documents in SharePoint Online are retained for eight years.

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

Correct Answer: See explanation below.

NB: For our purposes, the retention period will be 8 years.

For retaining email messages in Exchange Online:

Step 1: Create a retention tag

1.

Navigate to the Exchange Admin Center

2.

Navigate to Compliance management > Retention tags, and then click Add +

3.

Select one of the following options:

Applied automatically to entire mailbox (default): Select this option to create a default policy tag (DPT). You can use DPTs to create a default deletion policy and a default archive policy, which applies to all items in the mailbox.

Applied automatically to a specific folder: Select this option to create a retention policy tag (RPT) for a default folder such as Inbox or Deleted Items.

Applied by users to items and folders (Personal): Select this option to create personal tags. These tags allow Outlook and Outlook on the web (formerly known as Outlook Web App) users to apply archive or deletion settings to a message or folders that are different from the settings applied to the parent folder or the entire mailbox.

4.

The New retention tag page title and options will vary depending on the type of tag you selected. Complete the following fields:

Name: Enter a name for the retention tag. The tag name is for display purposes and doesn't have any impact on the folder or item a tag is applied to. Consider that the personal tags you provision for users are available in Outlook and Outlook

on the web.

Apply this tag to the following default folder: This option is available only if you selected Applied automatically to a specific folder.

Retention action: Select one of the following actions to be taken after the item reaches its retention period:

Delete and Allow Recovery: Select this action to delete items but allow users to recover them using the Recover Deleted



Items option in Outlook or Outlook on the web. Items are retained until the deleted item retention period configured for the mailbox database or the mailbox user is reached.

Permanently Delete: Select this option to permanently delete the item from the mailbox database.

Move to Archive: This action is available only if you're creating a DPT or a personal tag. Select this action to move items to the user's In-Place Archive.

Retention period: Select one of the following options:

Never: Select this option to specify that items should never be deleted or moved to the archive.

When the item reaches the following age (in days): Select this option and specify the number of days to retain items before they're moved or deleted. The retention age for all supported items except Calendar and Tasks is calculated from

the date an item is received or created. Retention age for Calendar and Tasks items is calculated from the end date.

Comment: User this optional field to enter any administrative notes or comments. The field isn't displayed to users.

Step 2: Create a retention policy

1.

Navigate to Compliance management > Retention policies, and then click Add +

2.

In New Retention Policy, complete the following fields:

Name: Enter a name for the retention policy.

Retention tags: Click Add + to select the tags you want to add to this retention policy.

A retention policy can contain the following tags:

One DPT with the Move to Archive action.

One DPT with the Delete and Allow Recovery or Permanently Delete actions.

One DPT for voice mail messages with the Delete and Allow Recovery or Permanently Delete actions.

One RPT per default folder such as Inbox to delete items.

Any number of personal tags.

Step 3: Apply a retention policy to mailbox users

After you create a retention policy, you must apply it to mailbox users. You can apply different retention policies to different set of users.

1.

Navigate to Recipients > Mailboxes.

2.



In the list view, use the Shift or Ctrl keys to select multiple mailboxes.

3.

In the details pane, click More options.

4.

Under Retention Policy, click Update.

5.

In Bulk Assign Retention Policy, select the retention policy you want to apply to the mailboxes, and then click Save.

For retaining documents in SharePoint Online

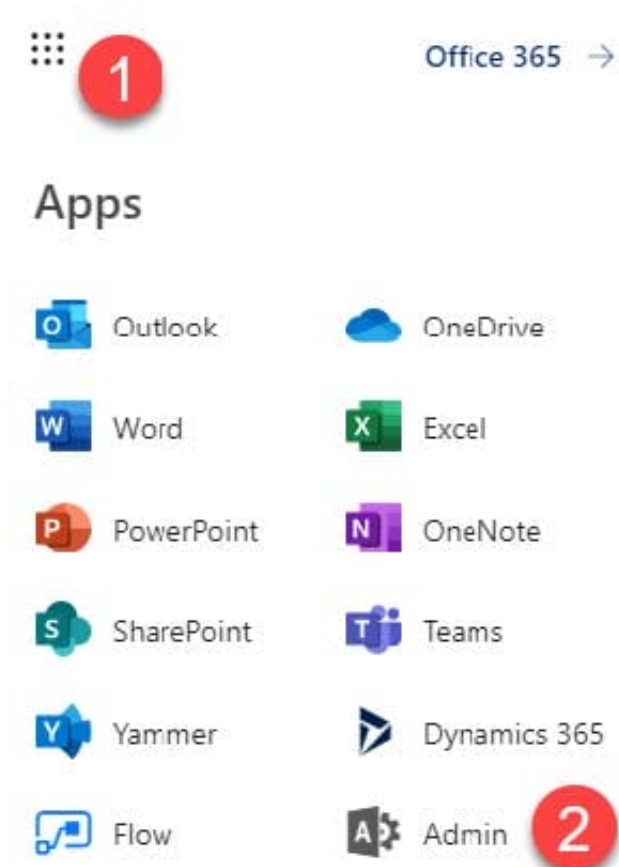
Access Security and Compliance Admin Center

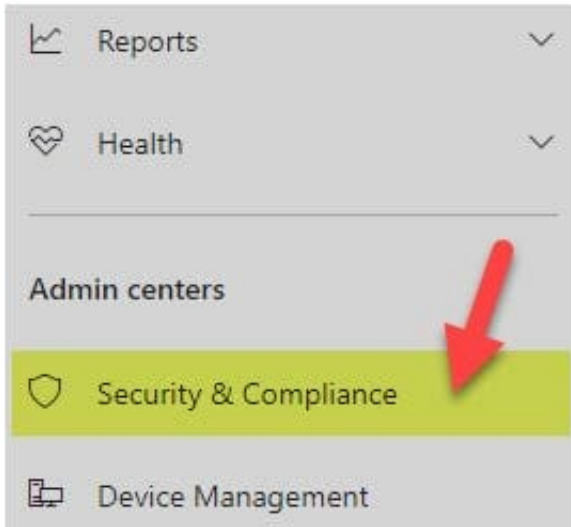
1.

Navigate to the Office 365 Admin Centers

2.

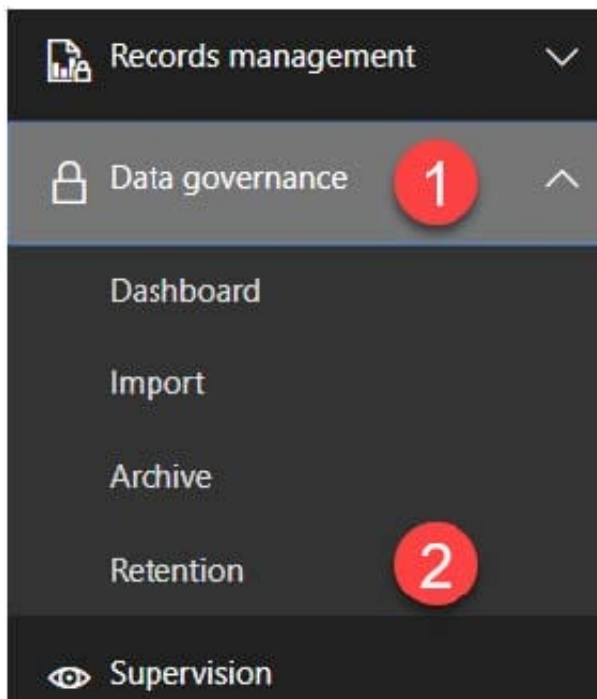
From the list of available Admin Centers, click on Security and Compliance





How to create and publish a Retention Policy on a SharePoint site

Now that we are in the Security and Compliance Admin Center, we are ready to create and publish a Retention Policy on a SharePoint site. Under Data Governance, click Retention




1. Hit Create button to create new Retention Policy



Home > Retention


Email, documents, Skype and Teams conversations. Your users generate a lot of content every day. Take control of it by setting up retention period of what you don't. [Learn more about retention](#)

Labels



Create labels to let users manually classify and retain their own content (email, docs, folders, and more). You can also auto-apply labels to specific content.

Label policies



Create label policies to publish or automatically apply existing labels to your users apps (Outlook, SharePoint, OneDrive, and more).

[+ Create](#) [Refresh](#) [...](#)

<input type="checkbox"/>	Name	Created by	Last modified ▼
<input type="checkbox"/>	3-day retention	Gregory Zelfond	September 9, 2019

2.

Give your policy a name and description. Hit Next

3.

On the next screen is where you set up the logic. You can configure how many days, months, or years to retain the content for, specify whether you want the math (retention period) to be calculated from the Created Date or Last Modified Date. Lastly, you can also specify whether you want to keep or delete content after the Retention period expires. Hit Next

4.

On the next screen, you get to choose where to apply the policy. You can apply it to email (Exchange), SharePoint sites, OneDrive accounts as well as Office 365 Groups.



Create a policy to retain what you want and get rid of what you don't.

Name your policy

Settings

Choose locations

Review your settings

Name your policy

Name * ⓘ

Retain for 2 days, then delete **1**

Description

This policy retains documents for 2 days after they were last modified and then deletes them **2**

3

Next

Cancel

Create a policy to retain what you want and get rid of what you don't.

Name your policy

Settings

Choose locations

Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 2 days **1**

Retain the content based on when it was last modified ⓘ **2**

Do you want us to delete it after this time? ⓘ

Yes No **3**

ⓘ At this time, creating a policy to delete Teams content that's less than 30 days old is not supported. If you want this policy to apply to Teams content, specify a retention period that's equal to or more than 30 days.

No, just delete content that's older than ⓘ

1 years

Need more options?

Use advanced retention settings ⓘ

4

Back

Next

Cancel



Create a policy to retain what you want and get rid of what you don't.

- ✓ Name your policy
- ✓ Settings
- Choose locations
- Review your settings

Choose locations

The policy will apply to content that's stored in the locations you choose.

- Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive and SharePoint documents
- Let me choose specific locations. ⓘ

Status	Location	Include	Exclude
<input type="checkbox"/>	Exchange email		
<input type="checkbox"/>	SharePoint sites		
<input type="checkbox"/>	OneDrive accounts		
<input checked="" type="checkbox"/>	Office 365 groups	All Choose groups	None Exclude groups

5. In my case, I applied a policy to a single Office 365 Group Site

Edit locations

1 group added

Choose groups

Groups (1) Clear all

Finance Team FinanceTeam@sharepointmaven.com



6. On a final screen, you need to review and confirm the settings and click Create this policy button. It is imperative to note the message you get to see at the bottom. It warns you that content might be deleted as soon as the policy takes effect according to the logic you set up in previous steps.

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings**

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name Edit
Retain for 2 days, then delete

Description Edit
This policy retains documents for 2 days after they were last modified and then deletes them

Applies to content in these locations Edit
SharePoint sites

Settings Edit
Retention period
Keep content, and delete it if it's older than 2 days

⚠ Content that's currently older than this will be deleted after you turn on the policy.

Back Save for later **Create this policy** Cancel

Reference:

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy#step-2-create-a-retention-policy>

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-retention-policy#use-the-eac-to-apply-a-retention-policy-to-multiple-mailboxes>

<https://sharepointmaven.com/how-to-set-a-retention-policy-on-a-sharepoint-site/>

QUESTION 8

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.



Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office 365	Assigned
Group14	Mail-enabled security group	Assigned

You create a sensitivity label named Label1.

You need to publish Label1.

To which groups can you publish Label1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On-premises Active Directory groups:

Group4 only	v
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	v
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12, Group13, and Group14	



Correct Answer:

Answer Area

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12, Group13, and Group14	

The groups must be mail-enabled.

Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

QUESTION 9

HOTSPOT

You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.

You need to ensure that you can add the security playbook and the custom query to the rule.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hot Area:

Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Correct Answer:



Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Box 1: Scheduled Create a custom analytics rule with a scheduled query

1.
From the Microsoft Sentinel navigation menu, select Analytics.
2.
In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.
3.
Etc.

Box 2: A trigger

Use triggers and actions in Microsoft Sentinel playbooks.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions#microsoft-sentinel-triggers-summary>

QUESTION 10



You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams.

You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

- A. Get-UnifiedGroup
- B. Get-MailUser
- C. Get-TeamMessagingSettings
- D. Get-TeamChannel

Correct Answer: A

<https://docs.microsoft.com/en-us/powershell/module/exchange/get-unifiedgroup?view=exchange-ps>

QUESTION 11

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

Name	Group	Role
User1	Group1	User administrator
User2	Group1	Security operator
User3	Group2	Security reader
User4	None	Global administrator

You enable self-service password reset for Group1 and configure security questions as the only authentication method for self-service password reset.

You need to identify which user must answer security questions to reset their password.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

Correct Answer: B



Self-service password reset (SSPR) is only enabled for Group1 (User1 and User2). User1 cannot use security questions for SSPR because User1 has an administrative security role. Therefore, only User2 can use SSPR with security questions as the authentication method.

References: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

QUESTION 12

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to ensure that User1 can review Conditional Access policies.

Solution: You assign User1 the Security Administrator role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 13

You have a Microsoft 365 E5 subscription that contains 100 users. Each user has a computer that runs Windows 10 and either an Android mobile device or an iOS mobile device. All the devices are registered with Azure Active Directory (Azure AD).

You enable passwordless authentication for all the users.

You need to ensure that the users can sign in to the subscription by using passwordless authentication.

What should you instruct the users to do on their mobile device first?

A. Install a device certificate.

B. Install a user certificate.

C. Install the Microsoft Authenticator app.

D. Register for self-service password reset (SSPR).

Correct Answer: C

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.

Note: Microsoft Authenticator App

You can allow your employee's phone to become a passwordless authentication method. You may already be using the Microsoft Authenticator App as a convenient multi-factor authentication option in addition to a password. You can also



use the Authenticator App as a passwordless option.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

QUESTION 14

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 questions 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 Security and Compliance 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.

You run the Set-AuditConfig -Workload Exchange command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

References: <https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps>

QUESTION 15

You have a Microsoft 365 E5 subscription that has Microsoft 365 Defender enabled.

You plan to deploy a third-party app named App1 that will receive alert data from Microsoft 365 Defender.

Which format will Microsoft 365 Defender use to send the alert data to App1?

A. JSON

B. ZIP

C. XML



D. CSV

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts?view=o365-worldwide>

[Latest MS-500 Dumps](#)

[MS-500 Practice Test](#)

[MS-500 Study Guide](#)