

# **Free Questions for SC-200**

**Shared by Irwin on 04-10-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type:** MultipleChoice

---

You have an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.csv that contains 10,000 rows.

You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Excel, you apply filters to the existing columns in File1.csv to reduce the number of rows, and then you perform the Get & Transform Data operations to parse the AuditData column.

Does this meet the requirement?

**Options:**

---

**A-** Yes

**B-** No

**Answer:**

---

B

## Question 2

---

**Question Type:** MultipleChoice

---

You have an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.csv that contains 10,000 rows.

You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Defender, you modify the search criteria of the audit search to reduce the number of returned records, and then you export the results. From Excel, you perform the Get & Transform Data operations by using the new export.

Does this meet the requirement?

**Options:**

---

A- Yes

B- No

**Answer:**

---

A

## Question 3

---

**Question Type: Hotspot**

---

You have an Azure Storage account that will be accessed by multiple Azure Functions apps during the development of an application.

You need to hide Microsoft Defender for Cloud alerts for the storage account.

Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Entity type: Azure Resource  
IP address  
Azure Resource  
Host  
User account

Field: Resource Id  
Name  
Resource Id  
Address  
Command line

## Question 4

Question Type: Hotspot

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You have the hunting query shown in the following exhibit.

```
Run | Time range: Set in query | Save | Share | New alert rule | Export | Pin to | Format query
1 AuditLogs
2 | where TimeGenerated >ago(7d)
3 | where OperationName == "Add user"
4 | project AddedTime = TimeGenerated, user = tostring(TargetResources[0].userPrincipalName)
5 | join (AzureActivity
6 | where OperationName == "Create role assignment"
7 | project OperationName, RoleAssignmentTime = TimeGenerated, user = Caller) on user
8 | project-away user1
9
```

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	Yes	No
The query will identify the role assignment of User2.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User3.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input type="radio"/>	<input type="radio"/>

#### Answer:

---

## Question 5

---

### Question Type: Hotspot

---

You have a Microsoft Sentinel workspace.

You plan to visualize data from Microsoft SharePoint Online and OneDrive sites.

You need to create a KQL query for the visual. The solution must meet the following requirements:

- \* Select all workloads as a single operation.
- \* Include two parameters named Operations and Users.
- \* In the results, exclude empty values for the site URLs.

How should you complete the query? To answer, select the appropriate options in the answer area.

a. NOTE: Each correct selection is worth one point.

Answer Area

officeActivity

Answer:

- | where Operation in ((Operations))
- | where Operation in ((Operations))
- | where Operation in ((Operations))
- | where ("{Operations}"=="All" or (Operations))
- | where "{Operations:label}"=="All" or Operation in ((Operations))

Question 6

Question Type: Hotspot

- | project Site\_Url
- | project Site\_Url
- | where Operation != "
- | where Site\_Url != "
- | where Site\_Url =~ "

You have an Azure subscription that contains 50 virtual machines.

You plan to deploy Microsoft [Defender for Cloud.

You need to enable agentless scanning for 40 virtual machines. The solution must create disk snapshots of the virtual machines and perform out-of-band analysis of the snapshots.

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

NOTE: Each correct selection is worth one point.

Answer Area

Select Defender plan:

- Defender CSPM
- Defender CSPM
- Resource Manager
- Storage

**Answer:**

To exclude specific virtual machines, use:

- Tagging
- A role-based access control (RBAC) assignment
- An Azure Policy assignment
- Tagging

## Question 7

**Question Type: Hotspot**

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.

You initiated a live response session on Device1.

You need to run a command that will download a 250-MB file named File1.exe from the live response library to Device1. The solution must ensure that File1.exe is downloaded as a background process.

How should you complete the live response command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Answer:

getfile	file1.exe	&
collect		\$
getfile		&
library		>
putfile		<

## Question 8

Question Type: Hotspot

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

You have the on-premises devices shown in the following table.

Name	Management state	Operating system
Device1	Onboarded to and managed by using Microsoft Defender for Endpoint	Windows Server 2022
Device2	Discovered by Microsoft Defender for Endpoint and unmanaged	Linux

malware. You need to recommend response actions that meet the

ices.

\* Do NOT affect the ability to control managed devices.

Which actions should you use for each device? To answer, select the appropriate options in the answer area.

a. NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Device1:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device**

## Question 9

Question Type: Hotspot

Device2:

- Isolate device only**
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

You have an on-premises datacenter that contains a custom web app named Appl. App1 uses Active Directory Domain Services (AD DS) authentication and is accessible by using Microsoft Entra application proxy.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You receive an alert that a user downloaded highly confidential documents.

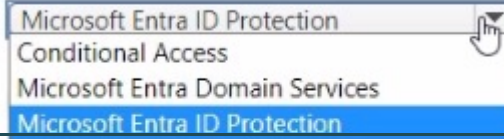
You need to remediate the risk associated with the alert by requiring multi-factor authentication (MFA) when users use App1 to initiate the download of documents that have a Highly Confidential sensitivity label applied.

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

NOTE: Each correct selection is worth one point.

## Answer Area

For App1 to require MFA, use:

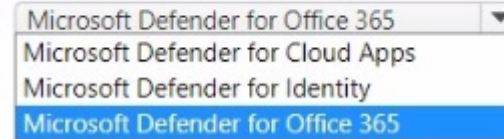


A screenshot of a dropdown menu with the following items: Microsoft Entra ID Protection, Conditional Access, Microsoft Entra Domain Services, and Microsoft Entra ID Protection. The second 'Microsoft Entra ID Protection' item is highlighted in blue. A mouse cursor is visible over the top-right corner of the menu.

**Answer:**

---

To implement a session policy, use:



A screenshot of a dropdown menu with the following items: Microsoft Defender for Office 365, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, and Microsoft Defender for Office 365. The last 'Microsoft Defender for Office 365' item is highlighted in blue.

## Question 10

---

**Question Type:** MultipleChoice

---

You have an Azure subscription.

You need to stream the Microsoft Graph activity logs to a third-party security information and event management (SIEM) tool. The solution must minimize administrative effort.

To where should you stream the logs?

### Options:

---

- A- an Azure Event Hubs namespace
- B- an Azure Event Grid namespace
- C- an Azure Storage account
- D- a Log Analytics workspace

**Answer:**

---

A

## Question 11

---

**Question Type:** MultipleChoice

---

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. You plan to create a Microsoft Defender XDR custom deception rule. You need to ensure that the rule will be applied to only 10 specific devices. What should you do first?

**Options:**

---

- A-** Add the IP address of each device to the list of decoy accounts and hosts of the rule.
- B-** Add the devices to a group.
- C-** Add custom lures to the rule.
- D-** Assign a tag to the devices

**Answer:**

---

B

## Question 12

---

### Question Type: MultipleChoice

---

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1. WS1 uses Microsoft Defender for Cloud.

You have the Microsoft security analytics rules shown in the following table.

Name	Service	Severity	Action
Rule1	Defender for Cloud	High	Create incident
Rule2	Defender for Cloud	High	Create incident
Rule3	Defender for Cloud	High	Create incident
Rule4	Defender for Cloud	High	Create incident

User1 performs an action that matches Rule1, Rule2, Rule3, and Rule4. How many incidents will be created in WS1?

### Options:

---

A- 1

B- 2

C- 3

D- 4

**Answer:**

---

A

**To Get Premium Files for SC-200 Visit**

**<https://www.p2pexams.com/products/sc-200>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/microsoft/pdf/sc-200>**

