



Free Questions for [SC-200](#) by [actualtestdumps](#)

Shared by [Hancock](#) on [15-04-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: Hotspot

You have a Microsoft Sentinel workspace that has a default data retention period of 30 days. The workspace contains two custom tables as shown in the following table.

Name	Table plan	Interactive retention	Total retention period
Table1	Basic	Default	Default
Table2	Analytics	Default	365

le.

Name	KQL statement
Query1	Table1 where TimeGenerated >= ago(15) summarize count(*)

the statement is true. Otherwise, select No.

Answer Area

Statements

Yes

No

For Query1 to return a value of 30, you must change Table plan to **Analytics**.

Answer:

For Query2 to return a value of 240, you must change Total retention period to **120 days**.

For Query3 to return 90 rows, you must change Total retention period to **45 days**.

Question 2

Question Type: MultipleChoice

You have a Microsoft 365 subscription that contains the following resources:

- * 100 users that are assigned a Microsoft 365 E5 license
- * 100 Windows 11 devices that are joined to the Microsoft Entra tenant

The users access their Microsoft Exchange Online mailbox by using Outlook on the web.

You need to ensure that if a user account is compromised, the Outlook on the web session token can be revoked.

What should you configure?

Options:

- A-** Microsoft Entra ID Protection
- B-** Microsoft Entra Verified ID
- C-** a Conditional Access policy in Microsoft Entra
- D-** security defaults in Microsoft Entra

Answer:

C

Question 3

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace named SW1.

In SW1, you investigate an incident that is associated with the following entities:

- * Host
- * IP address
- * User account
- * Malware name

Which entity can be labeled as an indicator of compromise (IoC) directly from the incident's page?

Options:

- A-** malware name
- B-** host
- C-** user account
- D-** IP address

Answer:

D

Question 4

Question Type: Hotspot

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You need to create a detection rule that meets the following requirements:

- * Is triggered when a device that has critical software vulnerabilities was active during the last hour
- * Limits the number of duplicate results

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

NOTE: Each correct selection is worth one point.

Answer Area

```
DeviceTvmSoftwareVulnerabilities  
| where VulnerabilitySeverityLevel == 'Critical'
```

Answer:

```
| distinct DeviceId  
| distinct Cveld  
| distinct DeviceId  
| project-away Cveld  
| project-keep DeviceId
```

Question 5

Question Type: Hotspot

```
| join kind=inner DeviceInfo on DeviceId  
| where Timestamp between (now(-1h)..now())
```

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

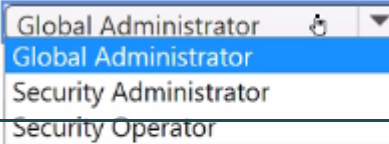
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for WS1. The solution must follow the principle of least privilege.

```
| project Timestamp, DeviceId, ReportId  
| distinct DeviceId  
| distinct DeviceId, ReportId  
| project Timestamp, DeviceId, ReportId  
| summarize count() by DeviceId, ReportId
```

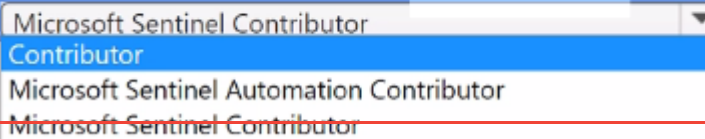
Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra role: 

Answer:

Role for WS1: 

Question 6

Question Type: Hotspot

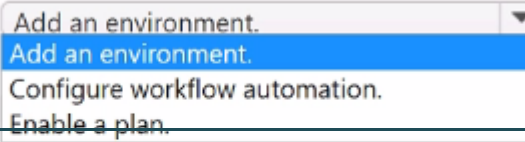
You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud.

You have an Azure DevOps organization named AzDO1.

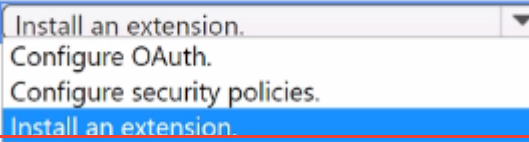
You need to integrate Sub1 and AzDO1. The solution must meet the following requirements:

- * Detect secrets exposed in pipelines by using Defender for Cloud.
- * Minimize administrative effort.

Answer Area

In Defender for Cloud:  Add an environment.
Add an environment.
Configure workflow automation.
Enable a plan.

Answer:

In AzDO1:  Install an extension.
Configure OAuth.
Configure security policies.
Install an extension.

Question 7

Question Type: Hotspot

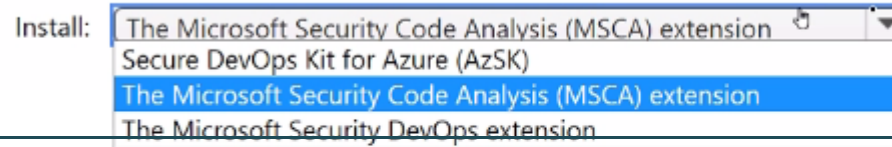
You have an Azure DevOps organization that uses Microsoft Defender for DevOps. The organization contains an Azure DevOps repository named Repo1 and an Azure Pipelines pipeline named Pipeline1. Pipeline1 is used to build and deploy code stored in Repo1.

You need to ensure that when Pipeline1 runs, Microsoft Defender for Cloud can perform secret scanning of the code in Repo1.

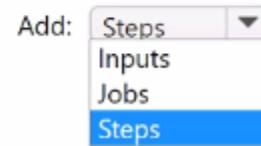
What should you install in the organization, and what should you add to the YAML file of Pipeline1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Question 8

Question Type: DragDrop

You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1. You need to ensure that the users can perform the following tasks in workspace1:

- * User1 must be able to dismiss incidents and assign incidents to users.
- * User2 must be able to modify analytics rules.

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

Contributor

Microsoft Sentinel Automation Contributor

Microsoft Sentinel Contributor

Microsoft Sentinel Reader

Microsoft Sentinel Responder

Reader

Answer Area

User1:

User2:

Question 9

Question Type: MultipleChoice

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps and has Cloud Discovery enabled.

You need to enrich the Cloud Discovery data.

a. The solution must ensure that usernames in the Cloud Discovery traffic logs are associated with the user principal name (UPN) of the corresponding Microsoft Entra ID user accounts.

What should you do first?

Options:

A- From Conditional Access App Control, configure User monitoring.

B- Create a Microsoft 365 app connector.

C- Enable automatic redirection to Microsoft 365 Defender.

D- Create an Azure app connector.

Answer:

B

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>

