SC-200Q&As

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

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

https://www.geekcert.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

You are informed of an increase in malicious email being received by users.

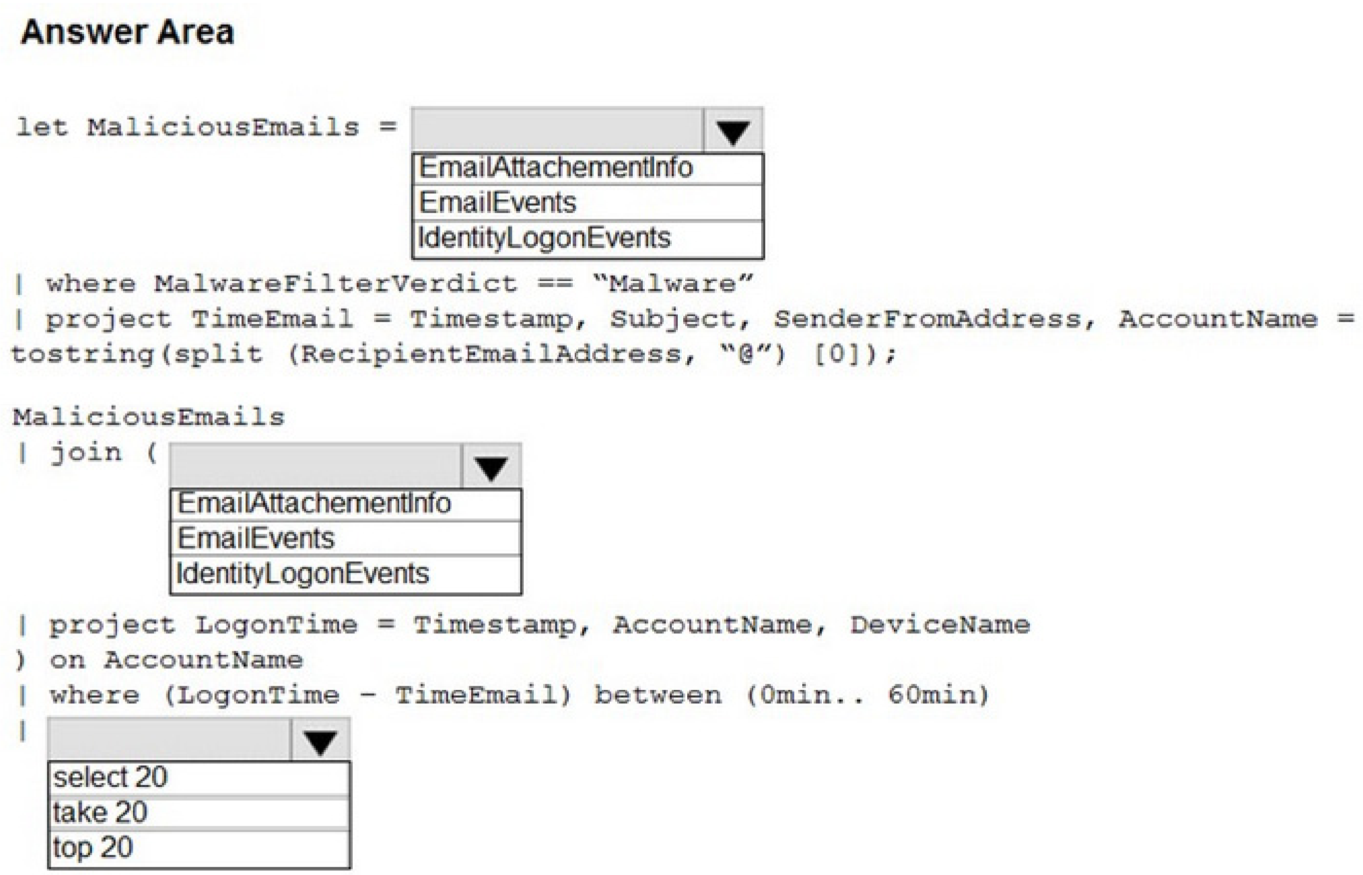
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an

hour of receiving the known malicious email.

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

NOTE: Each correct selection is worth one point.

Hot Area:

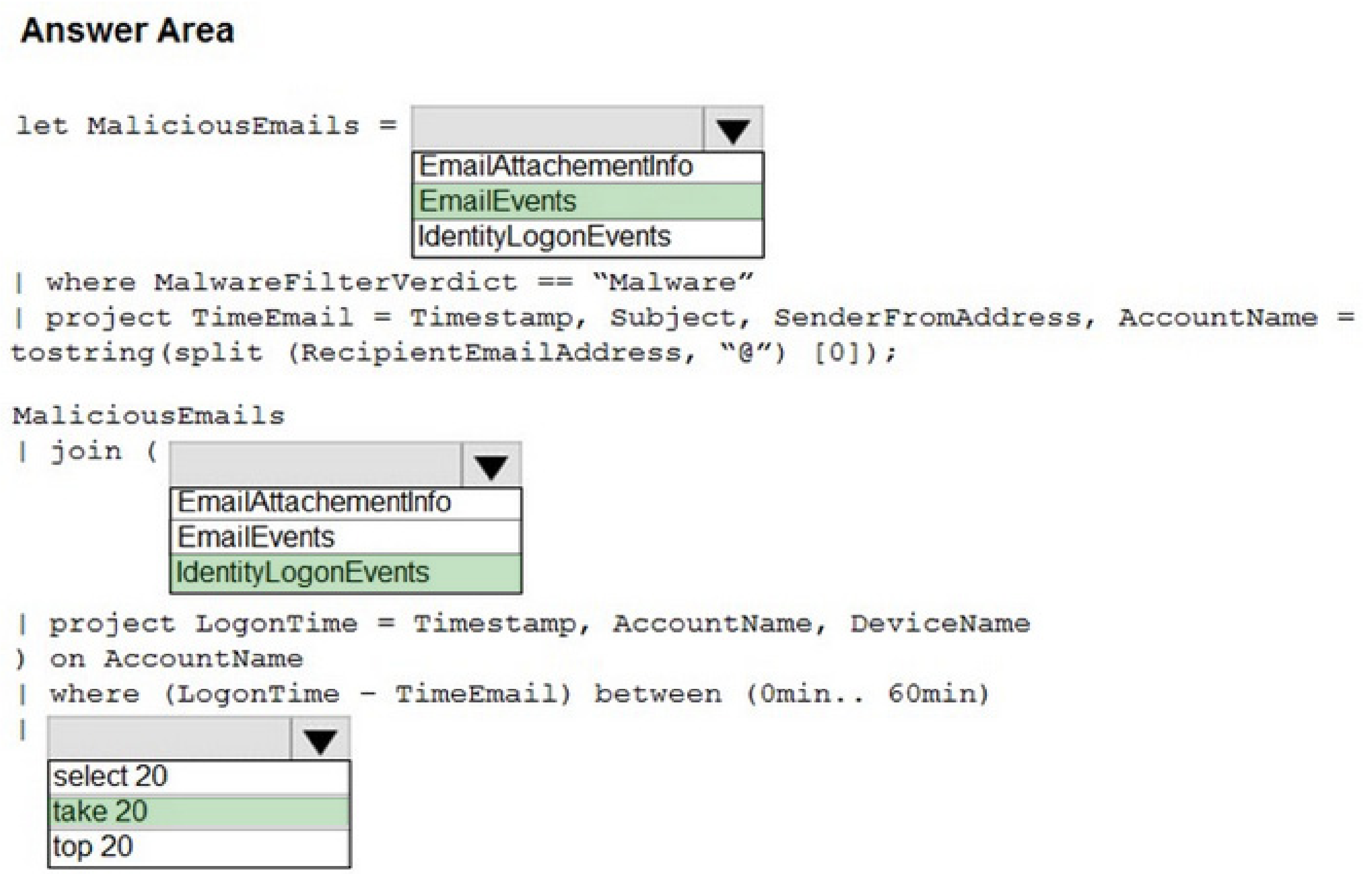


Answer Area

```
let MaliciousEmails = [▼ EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [▼ EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [▼ select 20 | take 20 | top 20]
```

Correct Answer:



Answer Area

```
let MaliciousEmails =
```

- EmailAttachementInfo
- [✓ EmailEvents]
- IdentityLogonEvents

```
| where MalwareFilterVerdict == “Malware”
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, “@”) [0]);

MaliciousEmails
| join (
```

- EmailAttachementInfo
- EmailEvents
- [✓ IdentityLogonEvents]

```
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
```

- select 20
- [✓ take 20]
- top 20

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

QUESTION 2

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.

You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

A. a file policy in Microsoft Defender for Cloud Apps

B. an access review policy

C. an alert policy in Microsoft Defender for Office 365

D. an insider risk policy

Correct Answer: C

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.

Default alert policies include:

Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files,

downloading files, and deleting files. This policy has a High severity setting.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

QUESTION 3

You have the following environment:

1.

Azure Sentinel

2.

A Microsoft 365 subscription

3.

Microsoft Defender for Identity

4.

An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.

You deploy Microsoft Defender for Identity by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified in Active Directory.

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

NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.

B. Modify the permissions of the Domain Controllers organizational unit (OU).

C. Configure auditing in the Microsoft 365 compliance center.

D. Configure Windows Event Forwarding on the domain controllers.

Correct Answer: AD

To enable auditing for sensitive groups, you need to configure the Advanced Audit Policy Configuration settings for the domain controllers. This can be done by modifying the Default Domain Controllers Policy in the Group Policy Management Console (GPMC) and enabling the "Audit Detailed Directory Service Replication" policy under "Advanced

Audit Policy Configuration\DS Access". This will generate audit events when sensitive groups are modified.

Windows Event Forwarding can be used to forward the audit events generated by the domain controllers to Azure Sentinel for analysis. This involves configuring a subscription on the domain controllers and a collection rule in Azure Sentinel to collect the forwarded events.

Reference: https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection
https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

You investigate a suspicious process named Prod on Device1 by using a live response session.

You need to perform the following actions:

1.

Stop Prod.

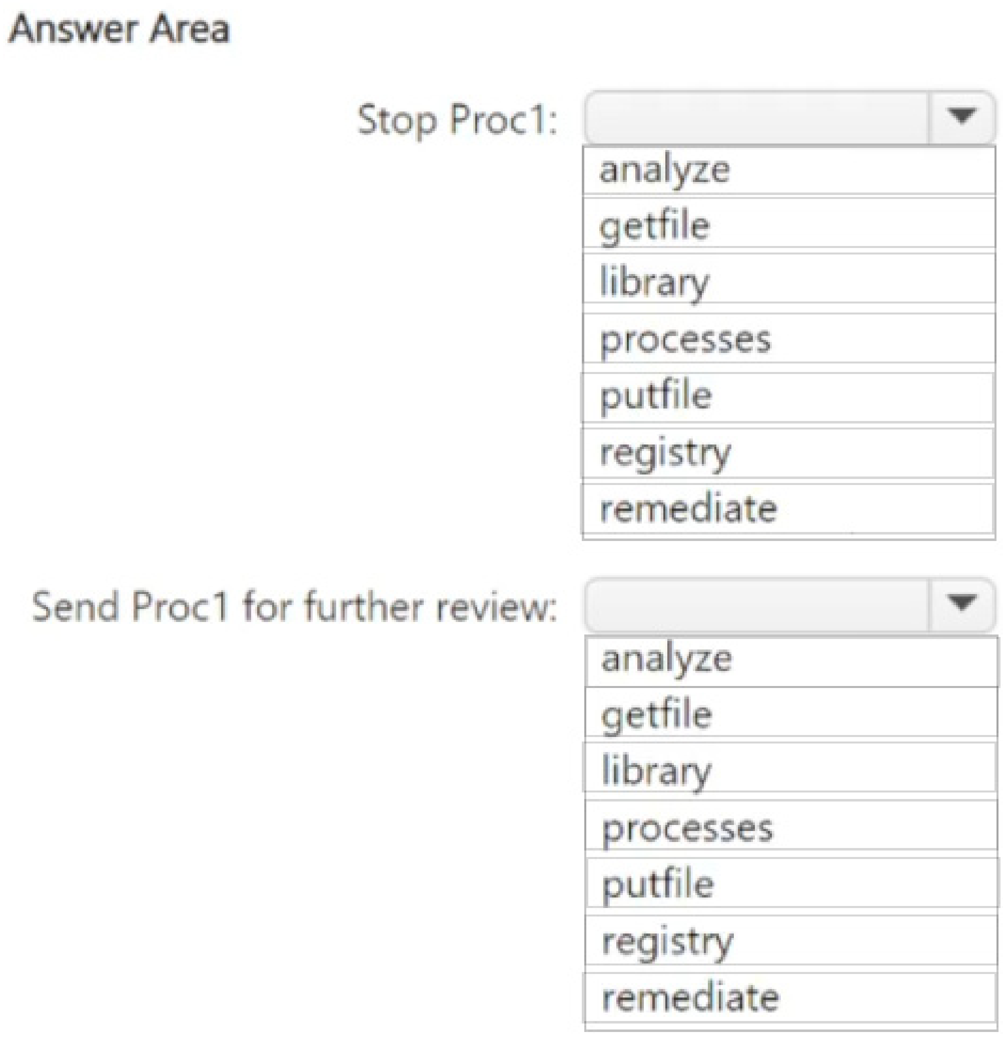
2.

Send Prod for further review.

Which live response command should you run for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

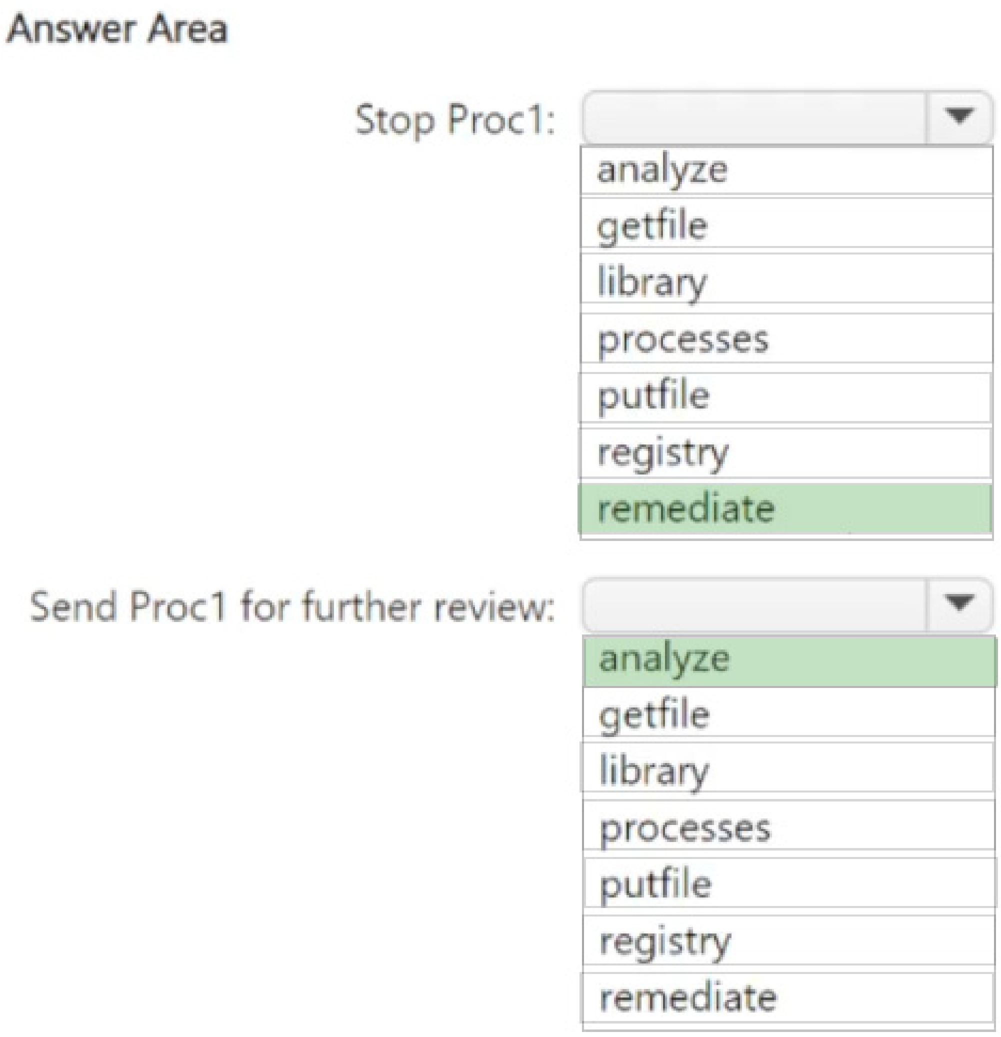


Answer Area

Stop Proc1:

Send Proc1 for further review:

Correct Answer:



Answer Area

Stop Proc1:

- analyze
- getfile
- library
- processes
- putfile
- registry
- [✓ remediate]

Send Proc1 for further review:

- [✓ analyze]
- getfile
- library
- processes
- putfile
- registry
- remediate

QUESTION 5

HOTSPOT

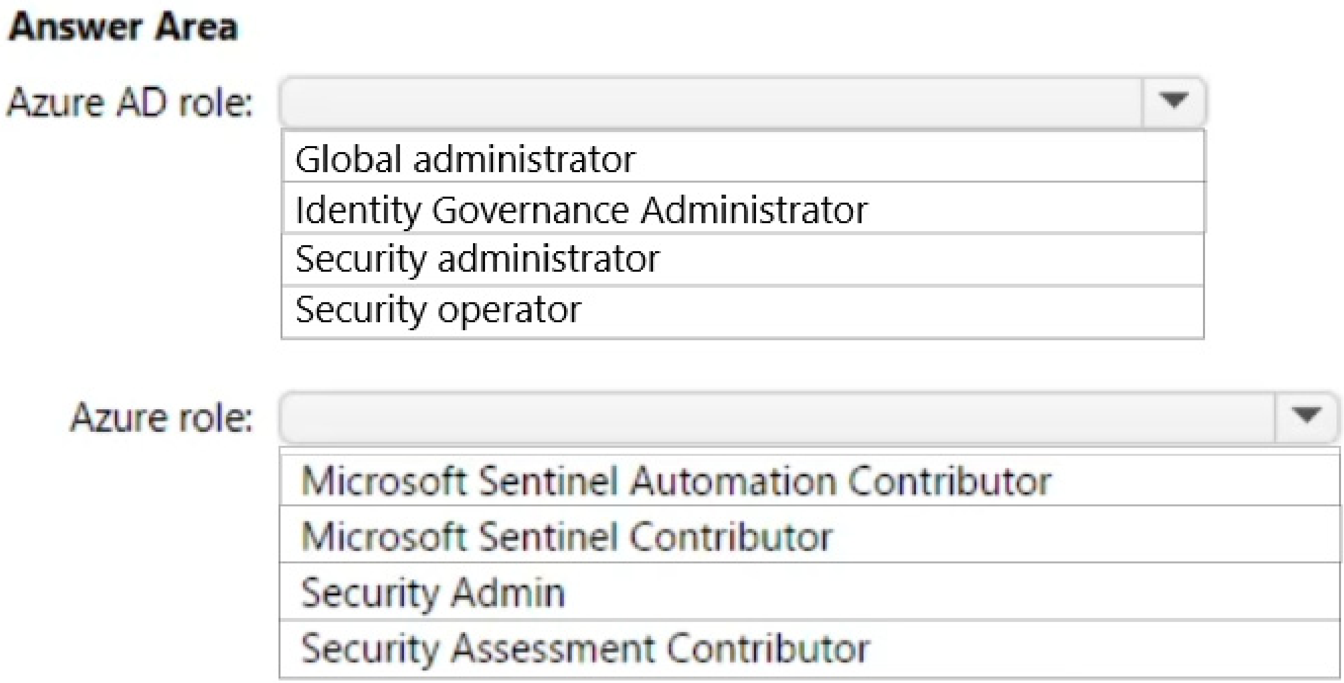
You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD. The solution must use the principle of least privilege.

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.

Hot Area:

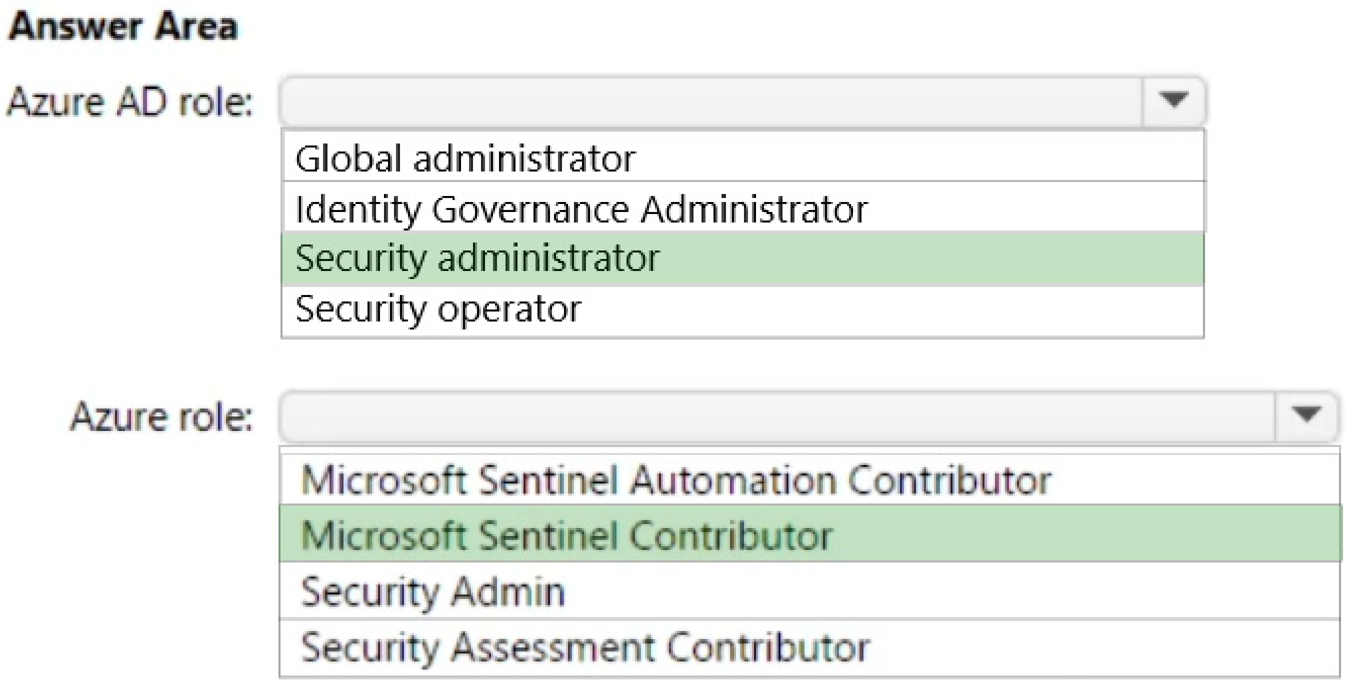


Answer Area

Azure AD role:
- Global administrator
- Identity Governance Administrator
- Security administrator
- Security operator

Azure role:
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor
- Security Admin
- Security Assessment Contributor

Correct Answer:



Answer Area

Azure AD role:
- Global administrator
- Identity Governance Administrator
- [✓ Security administrator]
- Security operator

Azure role:
- Microsoft Sentinel Automation Contributor
- [✓ Microsoft Sentinel Contributor]
- Security Admin
- Security Assessment Contributor

Box 1: Security Administrator

Azure AD Role

Enable User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

Prerequisites

To enable or disable this feature (these prerequisites are not required to use the feature):

Your user must be assigned the Global Administrator or Security Administrator roles in Azure AD.

Your user must be assigned at least one of the following Azure roles (Learn more about Azure RBAC):

Microsoft Sentinel Contributor at the workspace or resource group levels.

Log Analytics Contributor at the resource group or subscription levels.

Your workspace must not have any Azure resource locks applied to it. Learn more about Azure resource locking.

Box 2: Microsoft Sentinel Contributor

Azure Role

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics