SC-200 Q&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.certbus.com/sc-200.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 an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

A. Playbooks

B. Analytics

C. Threat intelligence

D. Incidents

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

QUESTION 2

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.

You are required to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user.

Which option should you use?

A. the Threat Protection Status report in Microsoft Defender for Office 365

B. the mail flow report in Exchange

C. the mailbox audit log in Exchange

D. the Safe Attachments file types report in Microsoft Defender for Office 365

Correct Answer: A

To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections). Reference:https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

QUESTION 3

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

A. Security solutions

B. Security policy

C. Pricing and settings

D. Security alerts

E. Azure Defender

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

QUESTION 4

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

You create a hunting query that detects a new attack vector. The attack vector maps to a tactic listed in the MITRE ATTandCK database.

You need to ensure that an incident is created in WS1 when the new attack vector is detected.

What should you configure?

A. a hunting livestream session

B. a query bookmark

C. a scheduled query rule

D. a Fusion rule

Correct Answer: C

QUESTION 5

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements. Which role should you assign?

A. Automation Operator

B. Automation Runbook Operator

C. Azure Sentinel Contributor

D. Logic App Contributor

Correct Answer: C

Litware must meet the following requirements:

1.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.

2.

The principle of least privilege must be used whenever possible.

Azure Sentinel Contributor can view data, incidents, workbooks, and other Azure Sentinel resources, manage incidents (assign, dismiss, etc.), create and edit workbooks, analytics rules, and other Azure Sentinel resources.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/roles

QUESTION 6

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

You are preparing an incident response plan for devices infected by malware. You need to recommend response actions that meet the following requirements:

1.

Block malware from communicating with and infecting managed devices.

2.

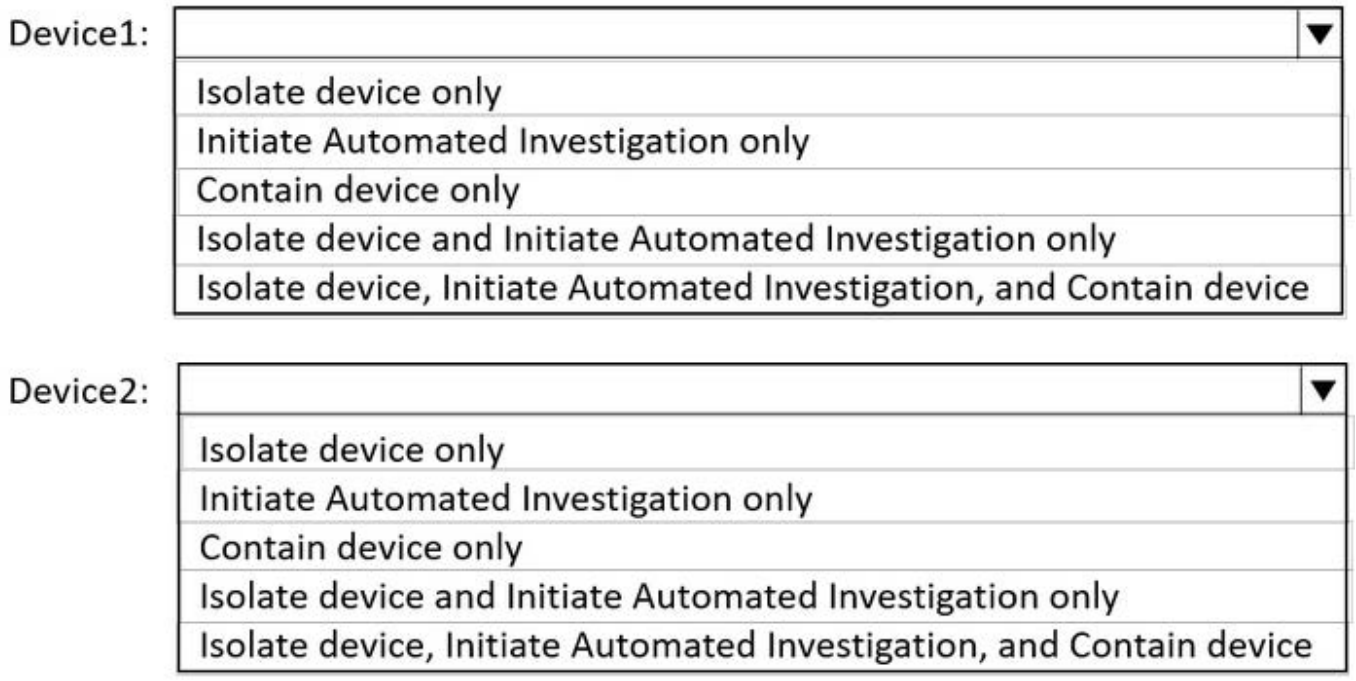
Do NOT affect the ability to control managed devices.

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

NOTE: Each correct selection is worth one point.

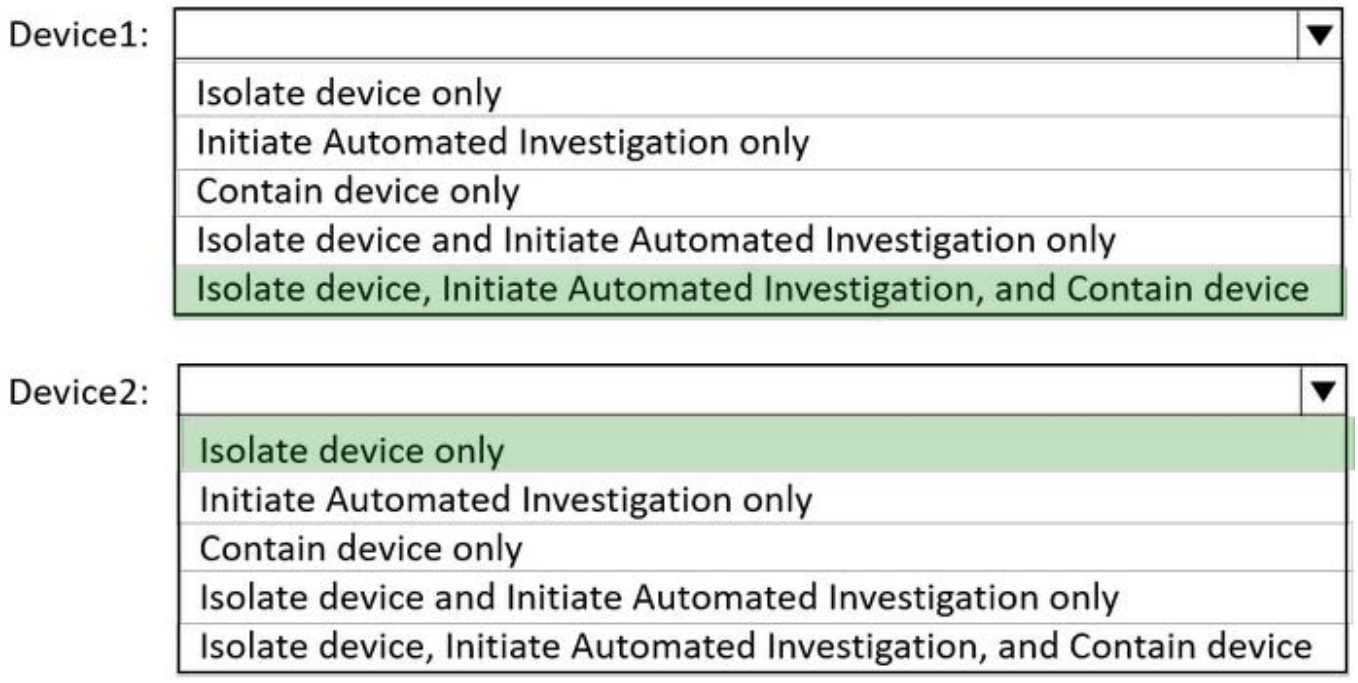
Hot Area:

Answer Area



Correct Answer:

Answer Area



QUESTION 7

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

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

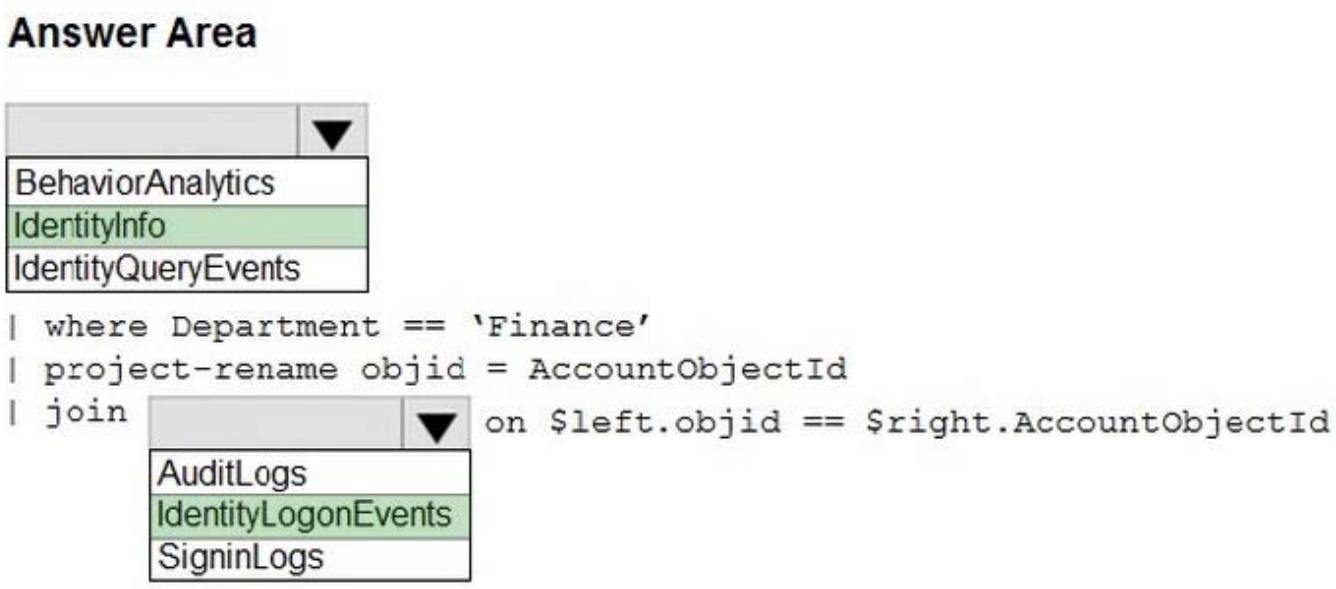
You need to identify all the interactive authentication attempts by the users in the finance department of your company.

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.

Hot Area:

Correct Answer:



Box 1: IdentityInfo Example: IdentityInfo | where JobTitle == "CONSULTANT" | join hint.shufflekey = AccountObjectId (IdentityDirectoryEvents

| where Application == "Active Directory" | where ActionType == "Private data retrieval") on AccountObjectId

Note: The IdentityInfo table in the advanced hunting schema contains information about user accounts obtained from various services, including Azure Active Directory. Use this reference to construct queries that return information from this table.

AccountObjectId Unique identifier for the account in Azure AD

Department Name of the department that the account user belongs to

Box 2: IdentityLogonEvents The IdentityLogonEvents table in the advanced hunting schema contains information about authentication activities made through your on-premises Active Directory captured by Microsoft Defender for Identity and authentication activities related to Microsoft online services captured by Microsoft Defender for Cloud Apps.

Column names include:

AccountObjectId Unique identifier for the account in Azure AD

Etc.

Incorrect:

Audit Logs (User and group management activity)

SignInLogs (Authentication Activity)

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identityinfo-table https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identitylogonevents-table

---

QUESTION 8

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

A. Microsoft Sentinel - Incidents

B. Microsoft Sentinel - Workbooks

C. Microsoft Sentinel

D. Log Analytics workspaces

Correct Answer: A

When you open Microsoft Sentinel, you are presented with a list of all the workspaces to which you have access rights, across all selected tenants and subscriptions. To the left of each workspace name is a checkbox. Selecting the name of a single workspace will bring you into that workspace. To choose multiple workspaces, select all the corresponding checkboxes, and then select the View incidents button at the top of the page.

https://learn.microsoft.com/en-us/azure/sentinel/multiple-workspace-view

---

QUESTION 9

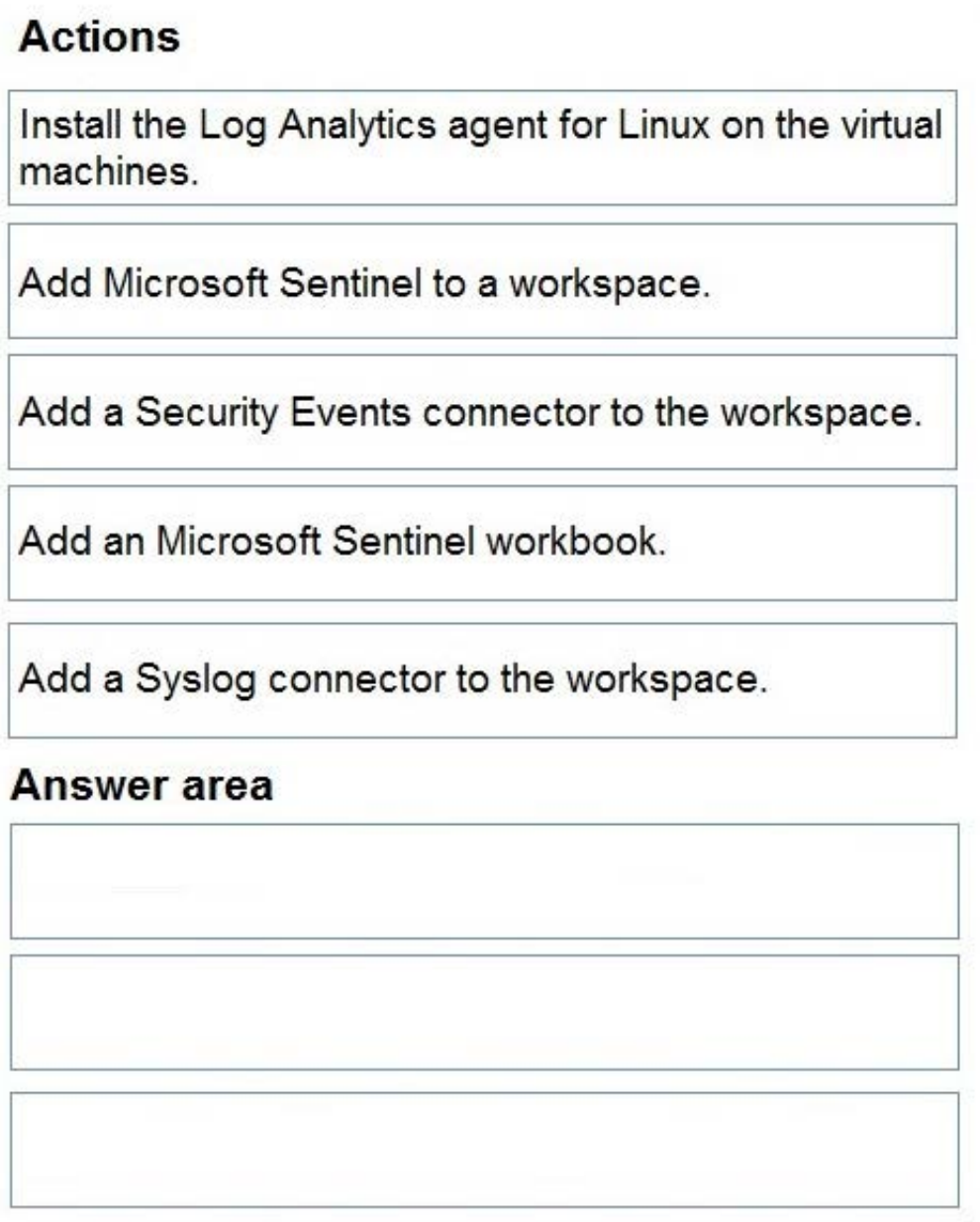
DRAG DROP

You have an Azure subscription that contains 100 Linux virtual machines.

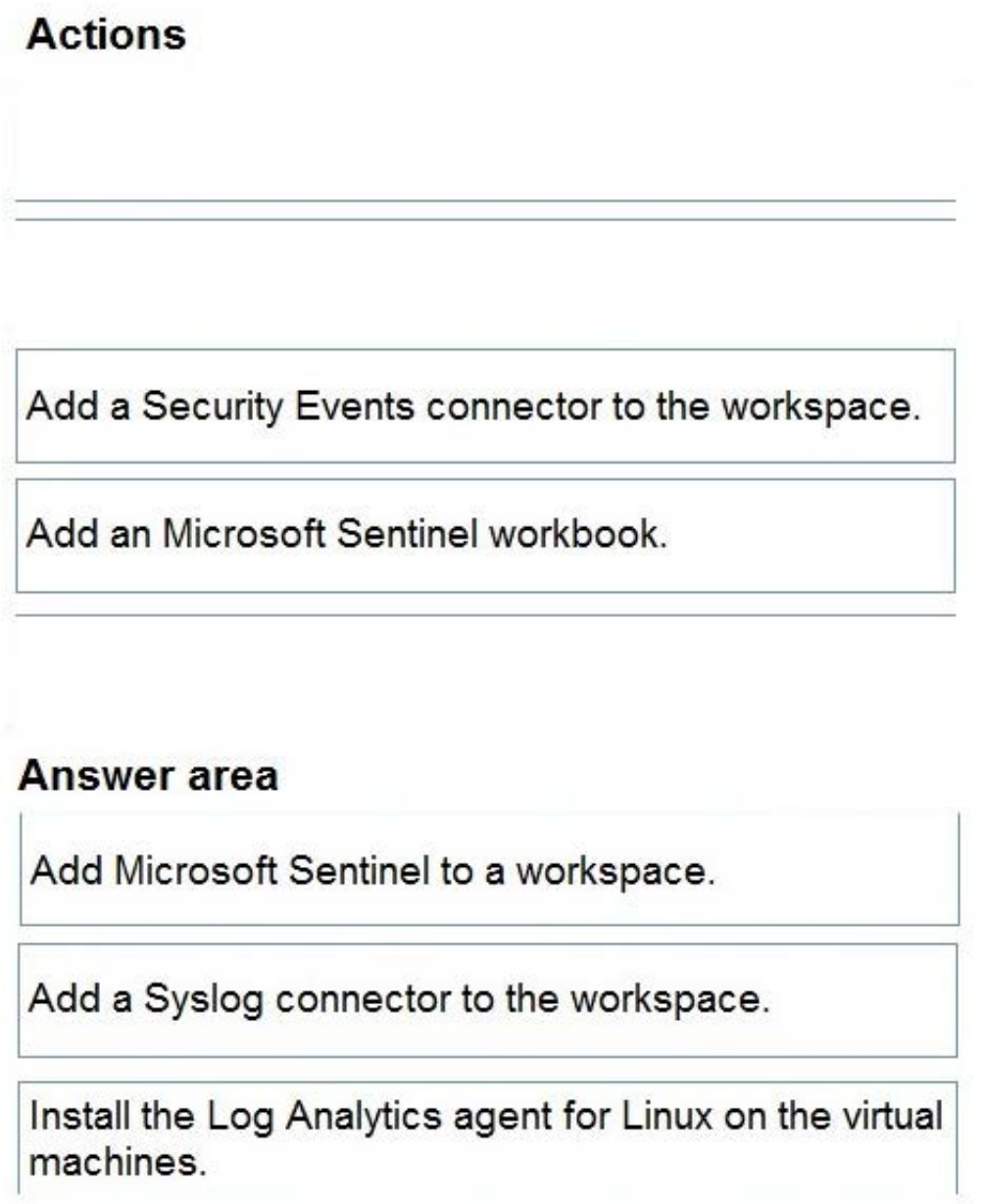
You need to configure Microsoft Sentinel to collect event logs from the virtual machines.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



QUESTION 10

You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center

B. Activity log in Azure

C. Azure Advisor

D. the query windows of the Log Analytics workspace

Correct Answer: D

QUESTION 11

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

A. Create a playbook.

B. Create a watchlist.

C. Create an analytics rule.

D. Add the query to a workbook.

Correct Answer: C

By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once

and it will run on a schedule, alerting you when the threat is detected.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule

QUESTION 12

HOTSPOT

You have an Azure subscription that uses Azure Defender.

You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set available effects to:

- Append
- DeployIfNotExists
- EnforceRegoPolicy

To perform remediation use:

- An Azure Automation runbook that has a webhook
- An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Correct Answer:

Answer Area

Set available effects to:

- Append
- DeployIfNotExists
- EnforceRegoPolicy

To perform remediation use:

- An Azure Automation runbook that has a webhook
- An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Reference: https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

QUESTION 13

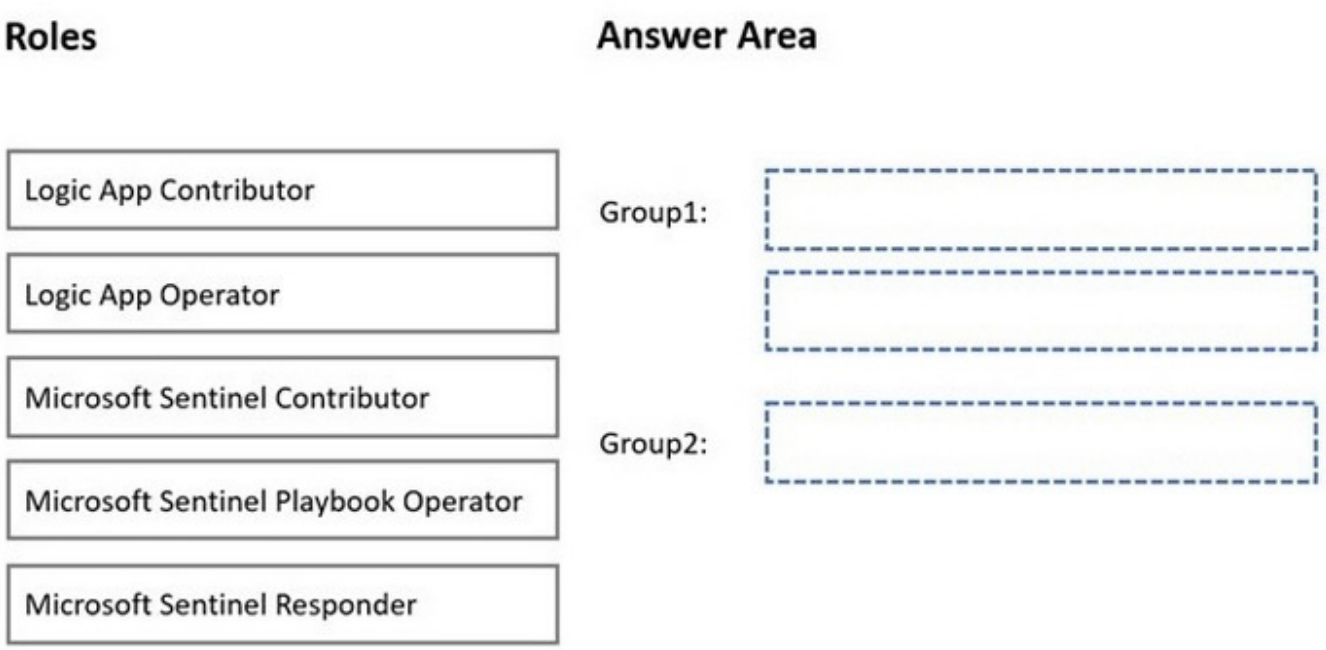
DRAG DROP

You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Sentinel requirements and the business requirements.

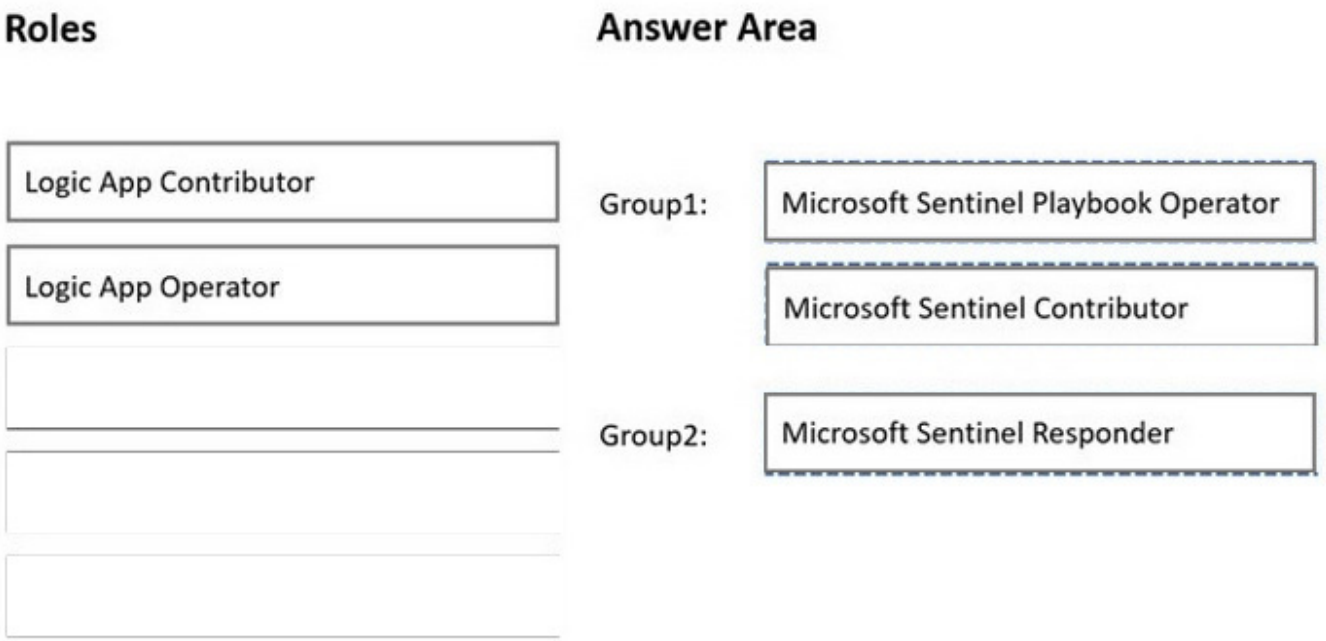
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Microsoft Sentinel Playbook Operator

Microsoft Sentinel Playbook Operator can list, view, and manually run playbooks.

Note: The fabrikam.com forest contains two global groups named Group1 and Group2.

Fabrikam identifies the following Microsoft Sentinel requirements:

Ensure that the members of Group1 can create and run playbooks.

Box 2: Microsoft Sentinel Contributor

Ensure that the members of Group1 can manage analytics rules.

Microsoft Sentinel Contributor can, in addition to the below (Microsoft Sentinel Reader +Microsoft Sentinel Responder), create and edit workbooks, analytics rules, and other Microsoft Sentinel resources.

Box 3: Microsoft Sentinel Responder

Ensure that the members of Group2 can manage incidents.

Microsoft Sentinel Reader can view data, incidents, workbooks, and other Microsoft Sentinel resources. Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.). Reference:

https://learn.microsoft.com/en-us/azure/sentinel/roles

QUESTION 14

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

A. Modify the access control settings for the key vault.

B. Enable the Key Vault firewall.

C. Create an application security group.

D. Modify the access policy for the key vault.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

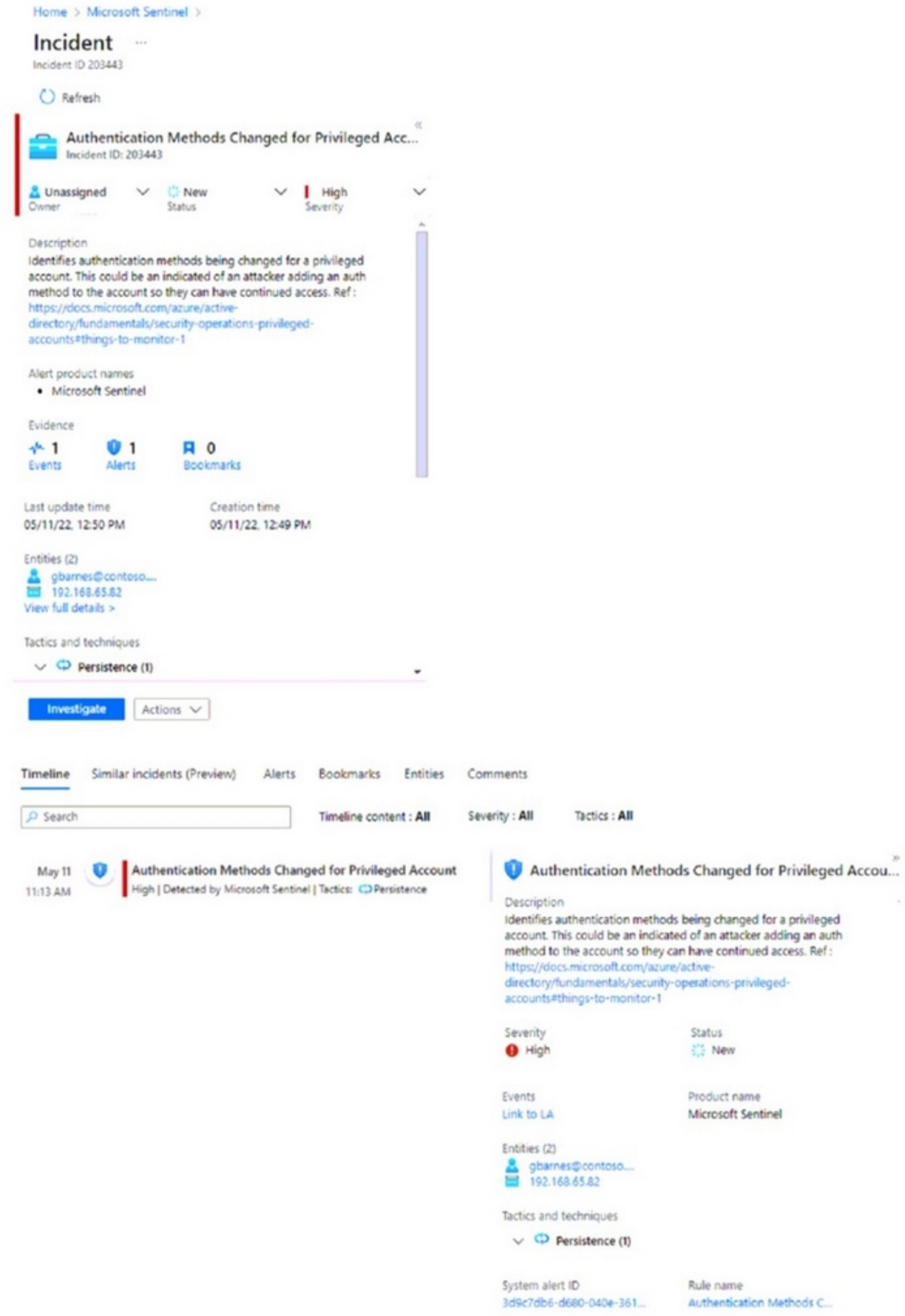
---

QUESTION 15

HOTSPOT

You have a Microsoft Sentinel workspace.

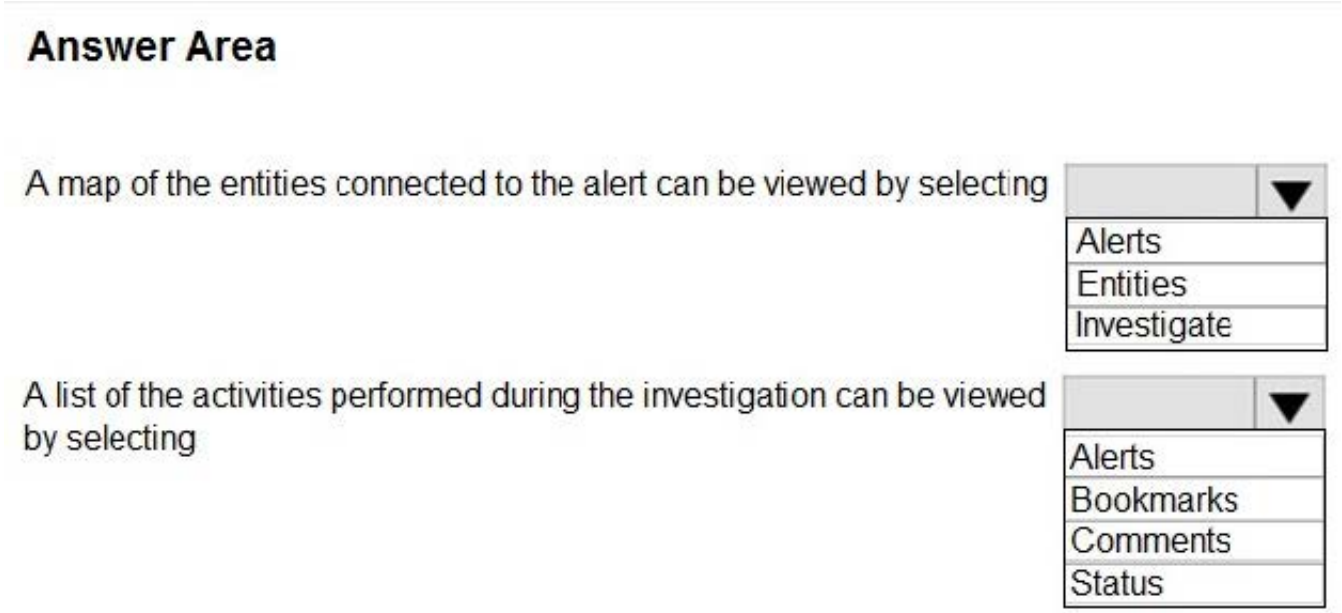
A Microsoft Sentinel incident is generated as shown in the following exhibit.


Home > Microsoft Sentinel >
Incident
Incident ID 203443
Refresh
Authentication Methods Changed for Privileged Acc...
Incident ID: 203443
Unassigned
Owner
New
Status
High
Severity
Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1
Alert product names
Microsoft Sentinel
Evidence
1 Events
1 Alerts
0 Bookmarks
Last update time
05/11/22, 12:50 PM
Creation time
05/11/22, 12:49 PM
Entities (2)
gbarnes@contoso....
192.168.65.82
View full details >
Tactics and techniques
Persistence (1)
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments
Search
Timeline content : All
Severity : All
Tactics : All
May 11
11:13 AM
Authentication Methods Changed for Privileged Account
High | Detected by Microsoft Sentinel | Tactics: Persistence
Authentication Methods Changed for Privileged Accou...
Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1
Severity
High
Status
New
Events
Link to LA
Product name
Microsoft Sentinel
Entities (2)
gbarnes@contoso....
192.168.65.82
Tactics and techniques
Persistence (1)
System alert ID
3d9c7db6-d680-040e-361...
Rule name
Authentication Methods C...

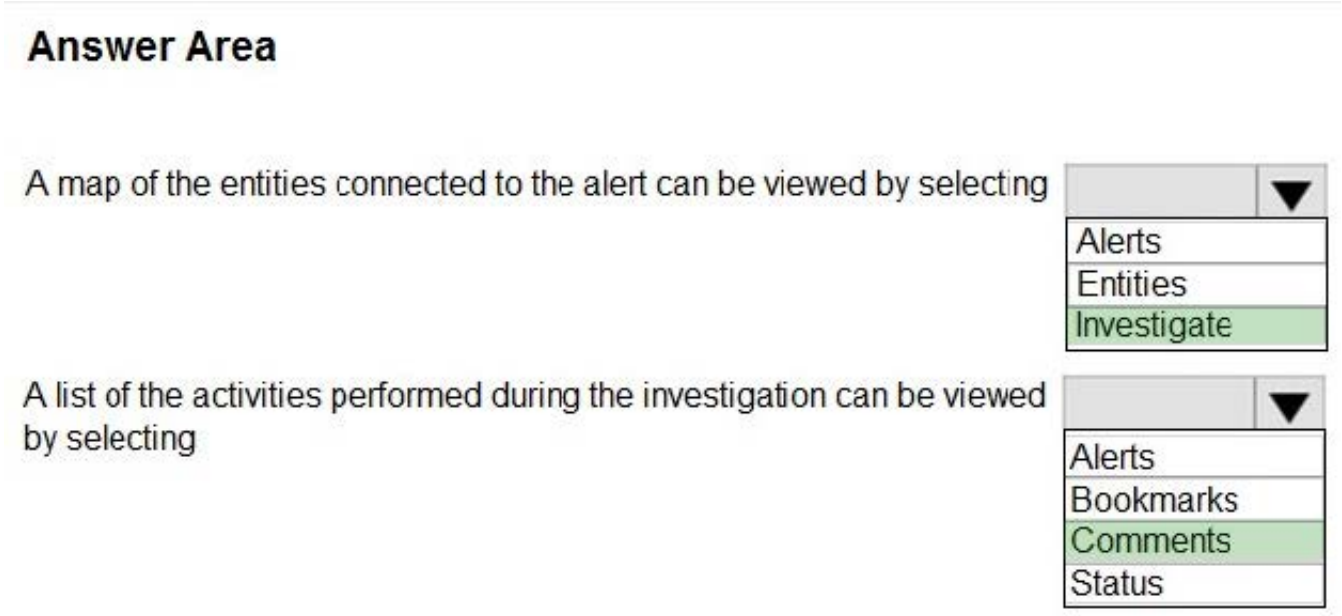
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Investigate

1.

To begin an investigation, select a specific incident. On the right, you can see detailed information for the incident including its severity, summary of the number of entities involved, the raw events that triggered this incident, the incident\\'s unique ID, and any mapped MITRE ATTandCK tactics or techniques.

2.

To view more details about the alerts and entities in the incident, select View full details in the incident page and review the relevant tabs that summarize the incident information.

A page similar to the exhibit will be shown.

3.

Select Investigate to view the investigation map.

Incorrect:

Entities

In the Entities tab, you can see all the entities that you mapped as part of the alert rule definition. These are the objects that played a role in the incident, whether they be users, devices, addresses, files, or any other types.

Alerts

In the Alerts tab, review the alerts included in this incident. You\\'ll see all relevant information about the alerts