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.pass4itsure.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

DRAG DROP

You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

You need to delegate the following tasks:

1.

Enable Microsoft Defender for Servers on virtual machines.

2.

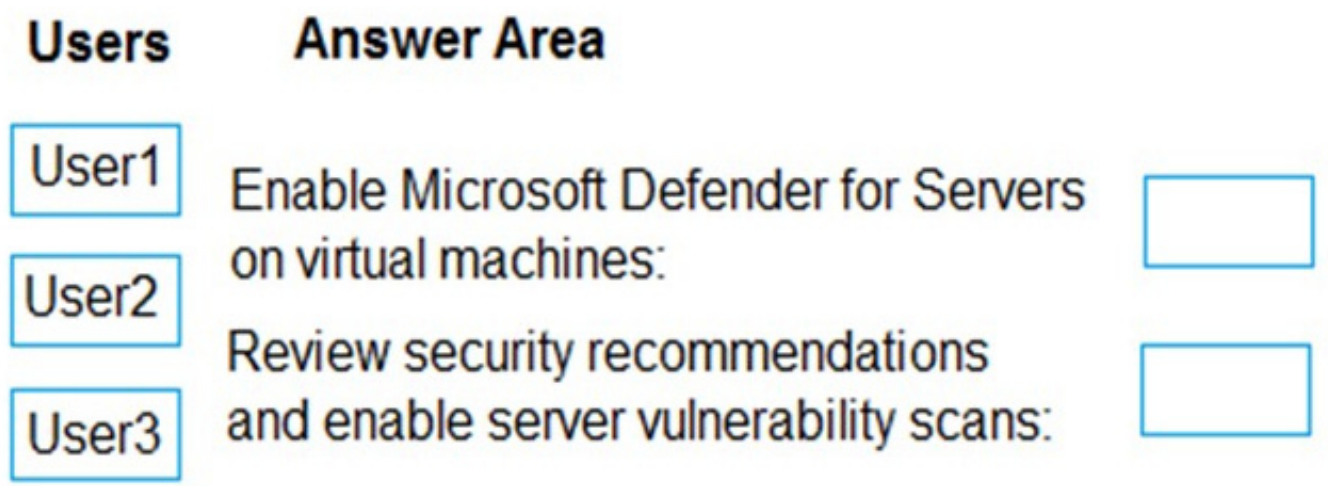
Review security recommendations and enable server vulnerability scans.

The solution must use the principle of least privilege.

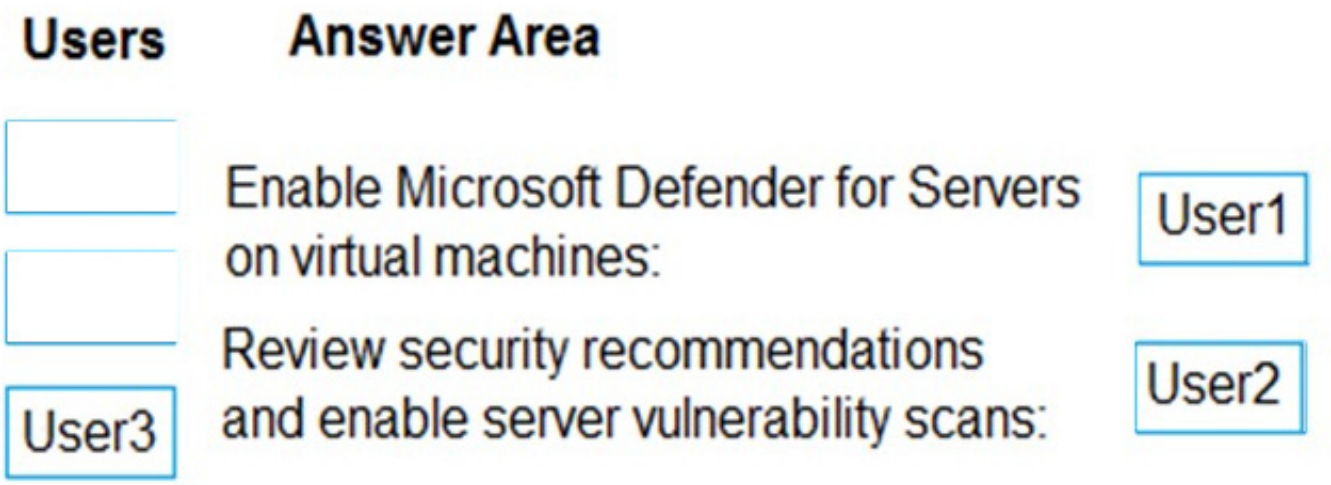
Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: User1

Enable Microsoft Defender for Servers on virtual machines.

User1 is Security Admin.

Security Admin

View and update permissions for Microsoft Defender for Cloud. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations.

Box 2: User2

Review security recommendations and enable server vulnerability scans.

User2 is Security Reader.

Security Reader

View permissions for Microsoft Defender for Cloud. Can view recommendations, alerts, a security policy, and security states, but cannot make changes.

Defender for Cloud\\'s integrated Qualys vulnerability scanner for Azure and hybrid machines

Required roles and permissions:

Owner (resource group level) can deploy the scanner

Security Reader can view findings

Incorrect:

Contributor (User3)

Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

Reference: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

QUESTION 2

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

What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

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

B. the mailbox audit log in Exchange

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

D. the mail flow report in Exchange

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

You have a Microsoft Sentinel workspace that contains the following incident.

Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident. What should you do?

A. From Overview, review the Potential malicious events map.

B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.

C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.

D. From Investigation, review insights on the incident entity.

Correct Answer: B

According to this article, Microsoft Defender for Cloud detects brute force attacks and triggers alerts that contain the attacking IP address in the ‘entities

QUESTION 4

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

A. Azure Synapse Analytics

B. Azure Machine Learning

C. Log Analytics

D. Azure Databricks

Correct Answer: B

Fabrikam identifies the following Microsoft Sentinel requirements:

Run hunting queries on Pool1 by using Jupyter notebooks.

Get started with Jupyter notebooks and MSTICPy in Microsoft Sentinel

Run and initialize the Getting Started Guide notebook

This procedure describes how to launch your notebook and initialize MSTICpy.

1.

In Microsoft Sentinel, select Notebooks from the left.

2.

From the Templates tab, select A Getting Started Guide For Microsoft Sentinel ML Notebooks > Save notebook to save it to your Azure ML workspace.

3.

Etc.

Reference: https://learn.microsoft.com/en-us/azure/sentinel/notebook-get-started

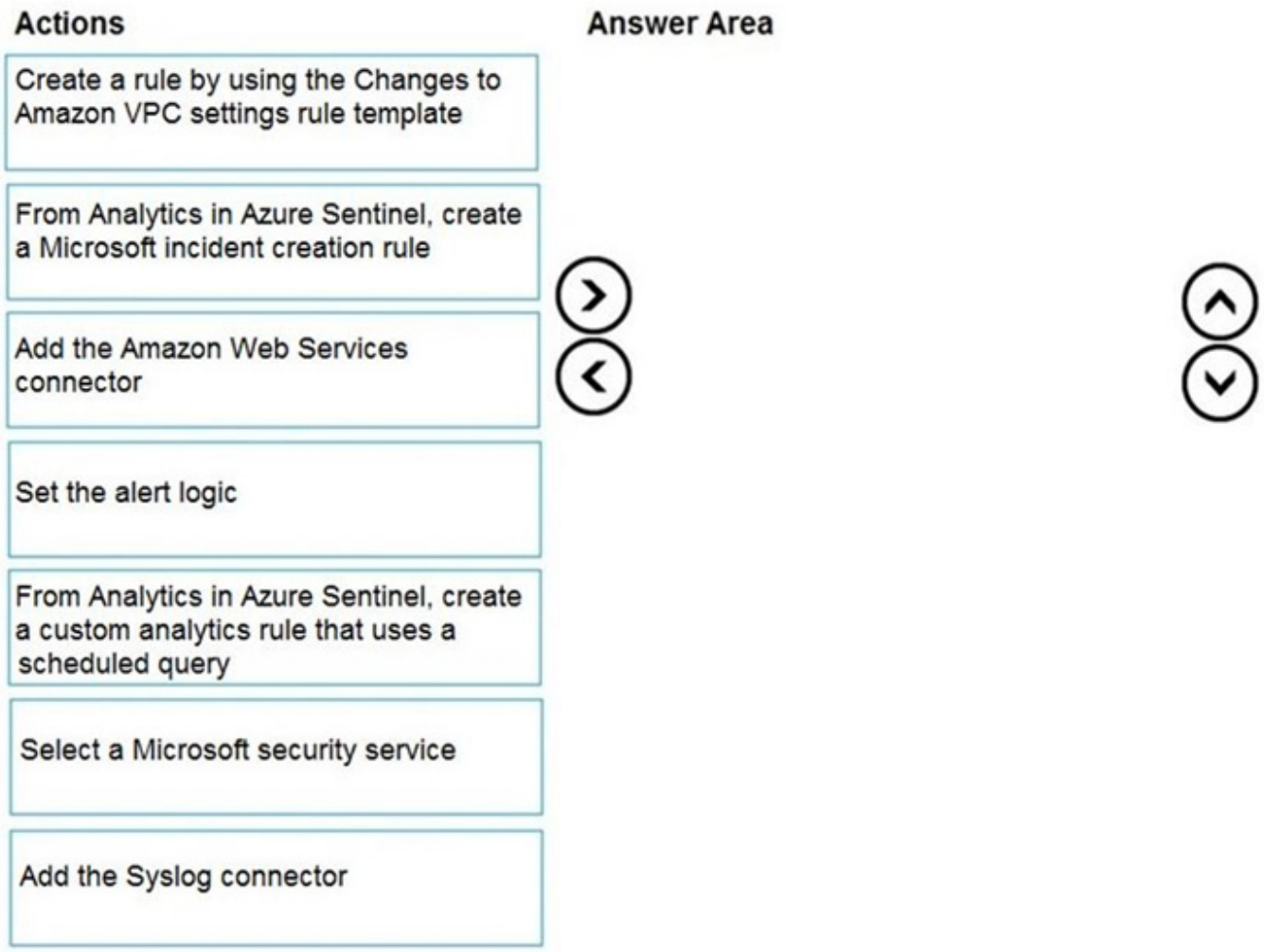
QUESTION 5

DRAG DROP

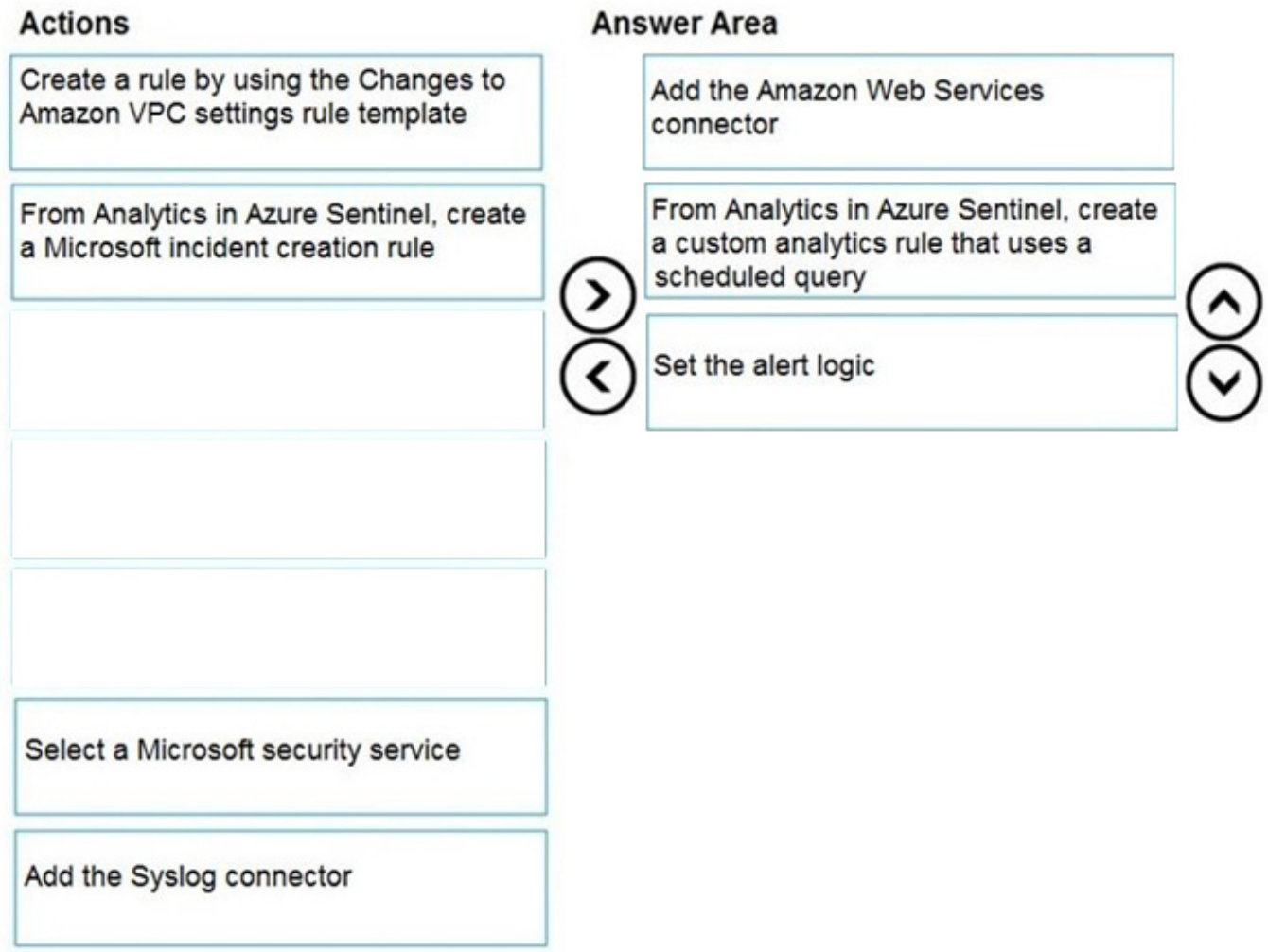
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

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:



Reference: https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

QUESTION 6

HOTSPOT

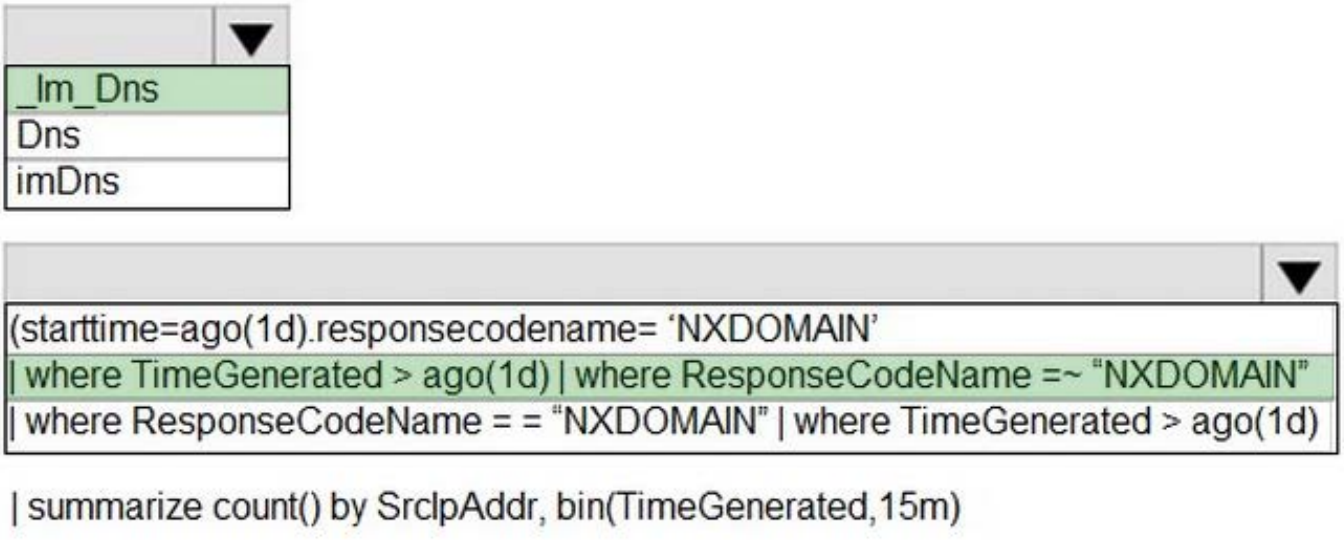
You have a Microsoft Sentinel workspace named Workspace1.

You configure Workspace1 to collect DNS events and deploy the Advanced Security Information Model (ASIM) unifying parser for the DNS schema.

You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN

Correct Answer:

Answer Area



Box 1: _Im_Dns

Example:

If your data source supports full DNS logging and you\\'ve chosen to log multiple segments, adjust your queries to prevent data duplication in Microsoft Sentinel.

For example, you might modify your query with the following normalization:

KQL

_Im_Dns | where SrcIpAddr != "127.0.0.1" and EventSubType == "response"

Box 2: | where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN" Example without filtering parameters would look like this:

Kusto

_Im_Dns | where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN" | summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

Incorrect:

(starttime=ago(1d), responsecodename=\\'NXDOMAIN\\'

Closing parantheses missing.

Correct would be: (starttime=ago(1d), responsecodename=\\'NXDOMAIN\\') as in the following code:

_Im_Dns(starttime=ago(1d), responsecodename=\\'NXDOMAIN\\') | summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

Reference: https://learn.microsoft.com/en-us/azure/sentinel/normalization-schema-dns

QUESTION 7

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

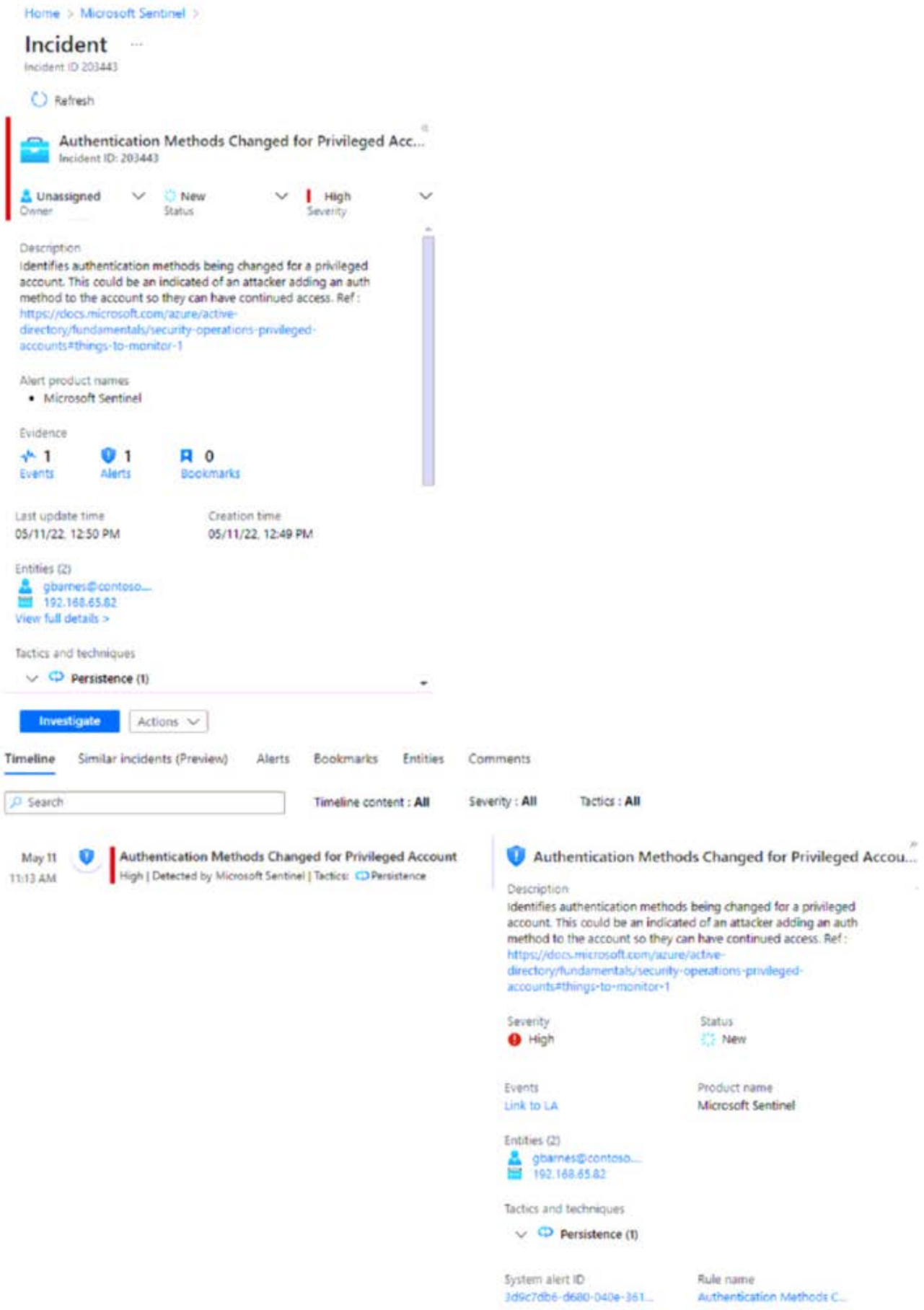
Correct Answer: C

QUESTION 8

HOTSPOT

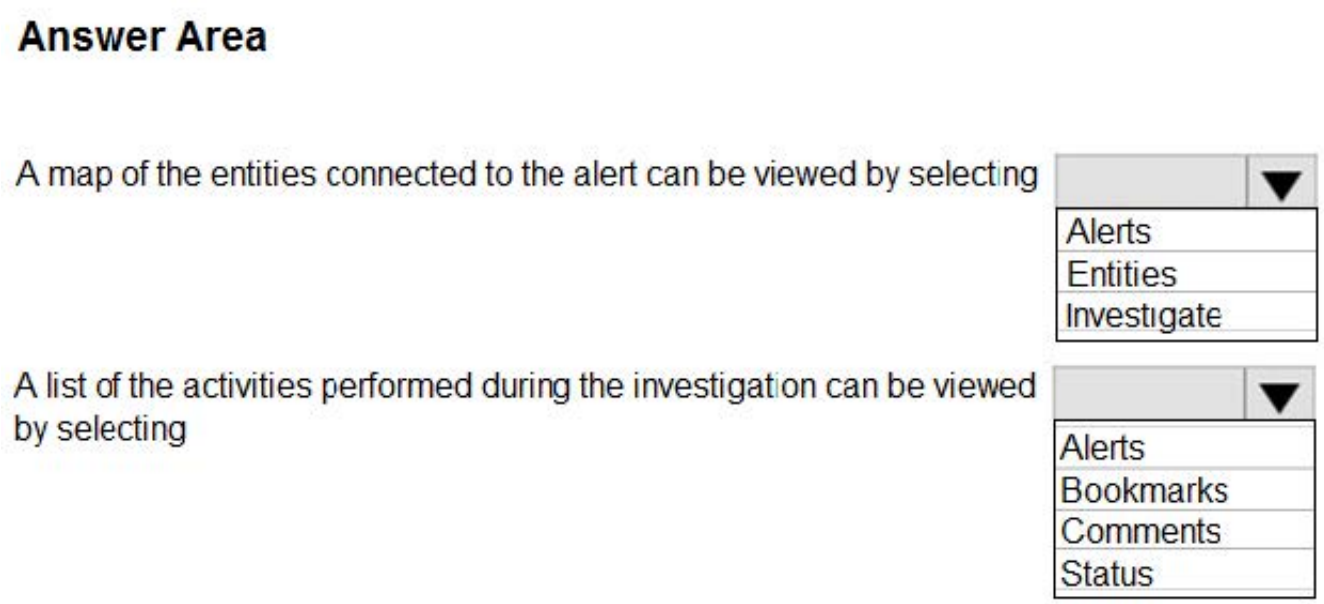
You have a Microsoft Sentinel workspace.

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

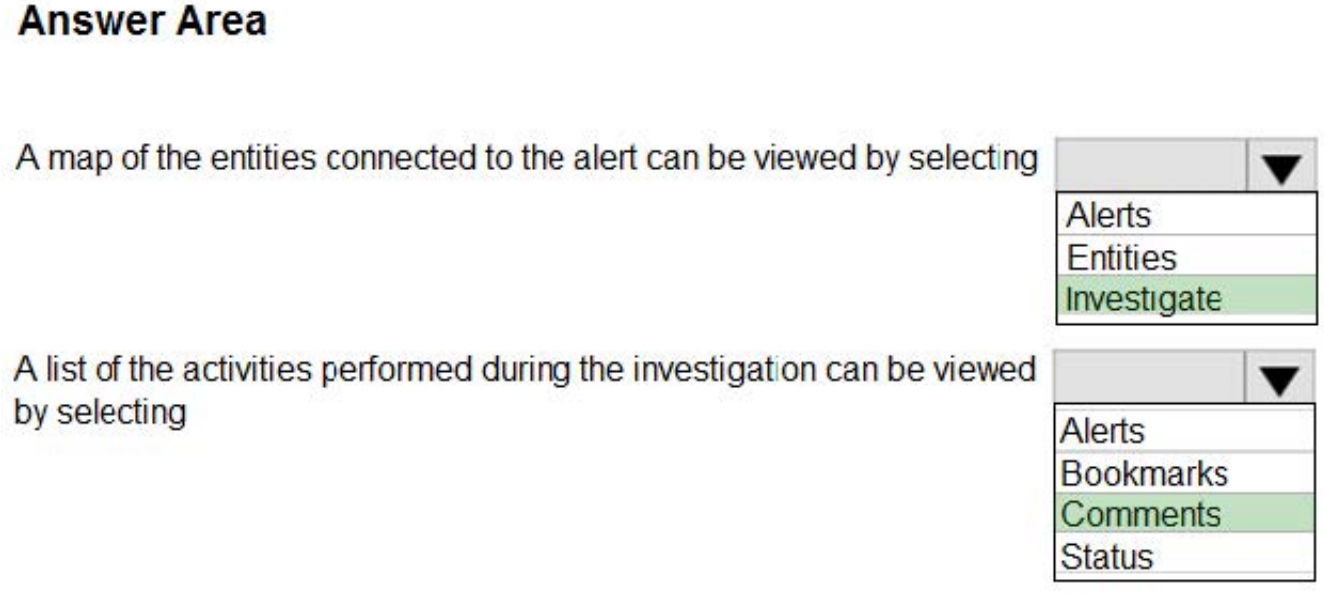

Home > Microsoft Sentinel >
Incident
Incident ID 203443
Refresh
Authentication Methods Changed for Privileged Acc...
Incident ID: 203443
Unassigned
Owner
New
Status
High
Severity
Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker 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:



QUESTION 9

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

You need to identify all the changes made to sensitivity labels during the past seven days.

What should you use?

A. the Incidents blade of the Microsoft 365 Defender portal

B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center

C. Activity explorer in the Microsoft 365 compliance center

D. the Explorer settings on the Email and collaboration blade of the Microsoft 365 Defender portal

Correct Answer: C

Labeling activities are available in Activity explorer.

For example:

Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.

It is captured at the time of save in Office native applications and web applications. It is captured at the time of occurrence in Azure Information protection add-ins. Upgrade and downgrade labels actions can also be monitored via the Label

event type field and filter.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide

QUESTION 10

You have five on-premises Linux servers.

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

You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

A. the Dependency agent

B. the Log Analytics agent

C. the Azure Connected Machine agent

D. the Guest Configuration extension

Correct Answer: C

The Azure Connected Machine agent is required to connect the on-premises Linux servers to the Azure subscription and integrate them with Microsoft Defender for Cloud. The agent enables communication between the servers and the Defender for Cloud service, allowing security events and data to be collected and analyzed.

Once the Azure Connected Machine agent is installed, you can then install the Log Analytics agent to collect security data from the servers and send it to the Log Analytics workspace in Azure. This will allow you to use Defender for Cloud

to monitor the security of your Linux servers, identify threats, and respond to security incidents.

QUESTION 11

HOTSPOT

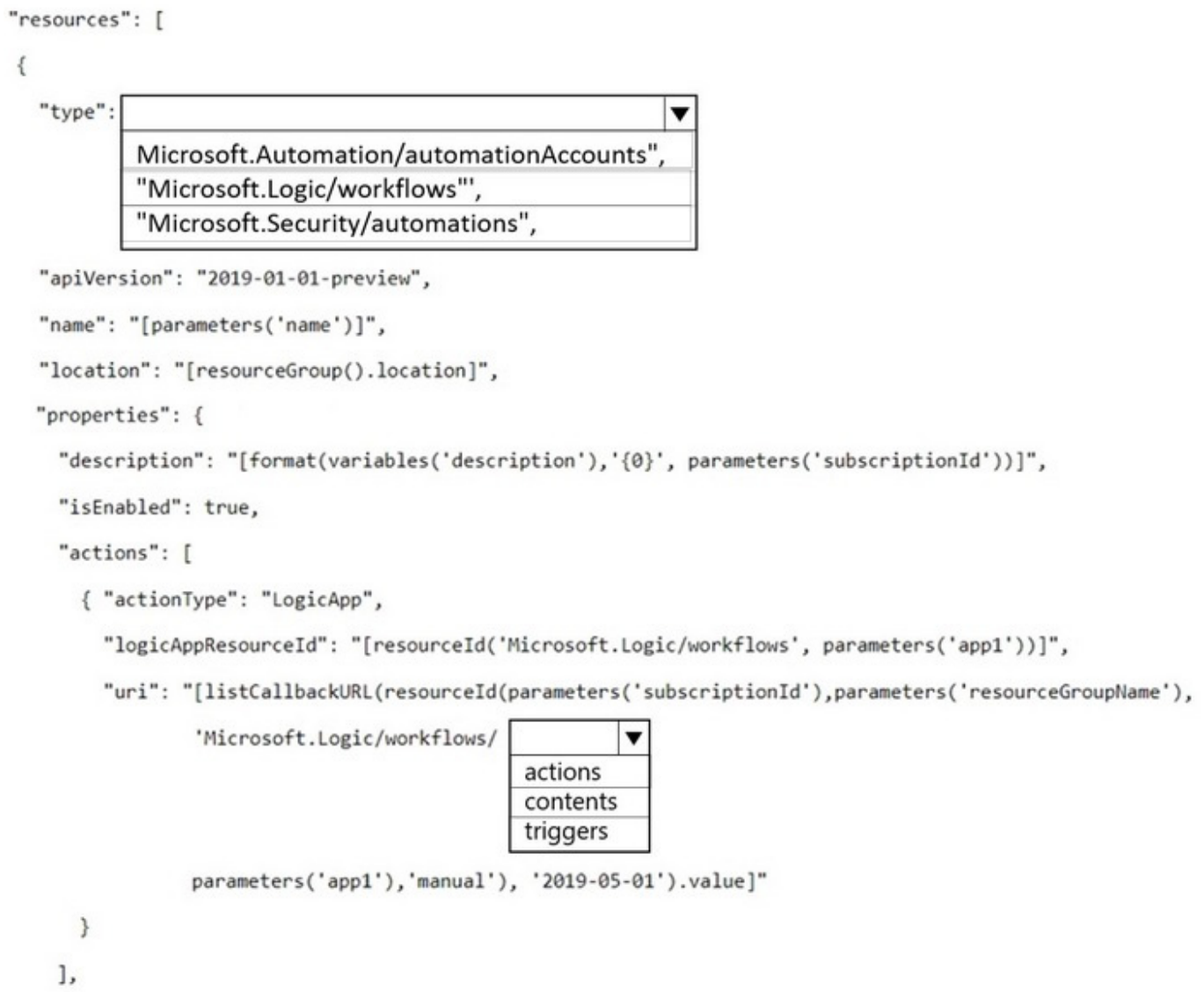
You have an Azure subscription that uses Microsoft Defender for Cloud and contains an Azure logic app named app1.

You need to ensure that app1 launches when a specific Defender for Cloud security alert is generated.

How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

```
"resources": [
 {
   "type":
```

Microsoft.Automation/automationAccounts",
"Microsoft.Logic/workflows"',
"Microsoft.Security/automations",

```
   "apiVersion": "2019-01-01-preview",
   "name": "[parameters('name')]",
   "location": "[resourceGroup().location]",
   "properties": {
     "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",
     "isEnabled": true,
     "actions": [
       { "actionType": "LogicApp",
         "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
         "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),
                 'Microsoft.Logic/workflows/
```

actions
contents
triggers

```
                 parameters('app1'),'manual'), '2019-05-01').value]"
       }
     ],
```

Box 1: “Microsoft.Security/automations"

Box 2: triggers Quickstart: Create an automatic response to a specific security alert using an ARM template or Bicep

Partial template: "resources": [

{

"type": "Microsoft.Security/automations",

"apiVersion": "2019-01-01-preview",

"name": "[parameters(\\'automationName\\')]",

"location": "[parameters(\\'location\\')]",

"properties": {

"description": "[format(variables(\\'automationDescription\\'), parameters(\\'subscriptionId\\'))]",

"isEnabled": true,

"actions": [

{ "actionType": "LogicApp", "logicAppResourceId": "[resourceId(\\'Microsoft.Logic/workflows\\', parameters(\\'logicAppName\\'))]", "uri": "[listCallbackURL(resourceId(parameters(\\'subscriptionId\\'), parameters(\\'logicAppResourceGroupName\\'), \\'Microsoft.Logic/workflows/triggers\\', parameters(\\'logicAppName\\'), \\'manual\\'), \\'2019-05-01\\').value]"

}

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-automation-alert?tabs=CLI

QUESTION 12

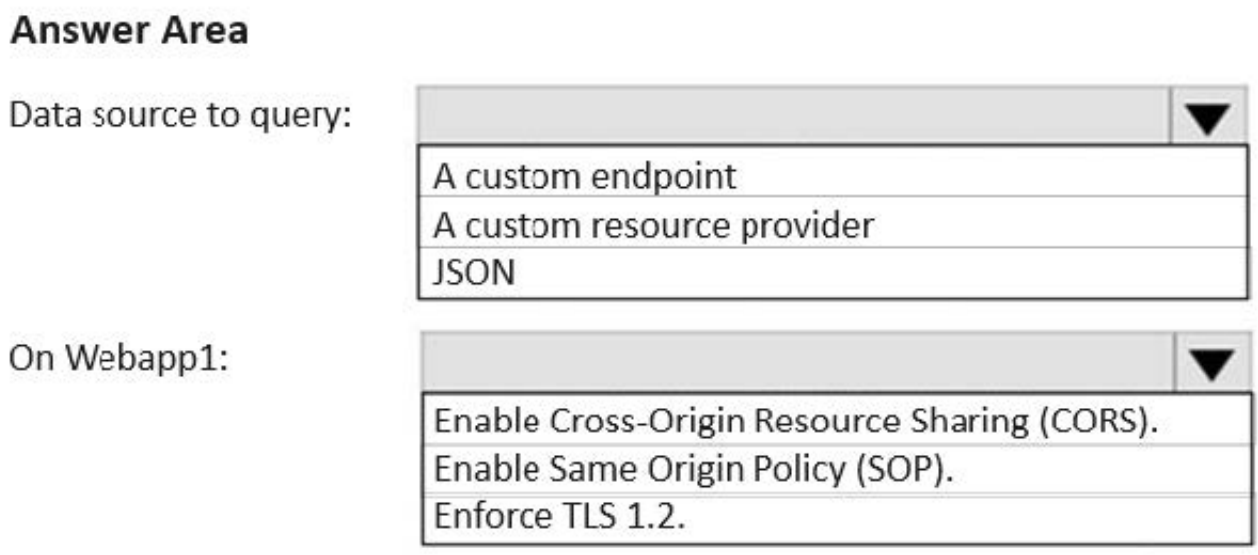
HOTSPOT

You need to implement the query for Workbook1 and Webapp1.

The solution must meet the Microsoft Sentinel requirements.

How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

Data source to query:

- A custom endpoint
- A custom resource provider
- JSON

On Webapp1:

- Enable Cross-Origin Resource Sharing (CORS).
- Enable Same Origin Policy (SOP).
- Enforce TLS 1.2.

QUESTION 13

HOTSPOT

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

You need to create a custom detection rule that will identify devices that had more than five antivirus detections within the last 24 hours.

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

```
DeviceEvents
| where ingestion_time() > ago(1d)
| where ActionType == "AntivirusDetection"
| summarize (Timestamp, [ DeviceId / InitiatingProcessAccountObjectId / ReportId / TimeGenerated ])=arg_max(Timestamp,
| where count_ > 5
), count() by [ DeviceId / InitiatingProcessAccountObjectId / ReportId / TimeGenerated ]
```

Correct Answer:

Answer Area

```
DeviceEvents
| where ingestion_time() > ago(1d)
| where ActionType == "AntivirusDetection"
| summarize (Timestamp, [ DeviceId / InitiatingProcessAccountObjectId / ReportId / TimeGenerated ])=arg_max(Timestamp,
| where count_ > 5
), count() by [ DeviceId / InitiatingProcessAccountObjectId / ReportId / TimeGenerated ]
```

QUESTION 14

HOTSPOT

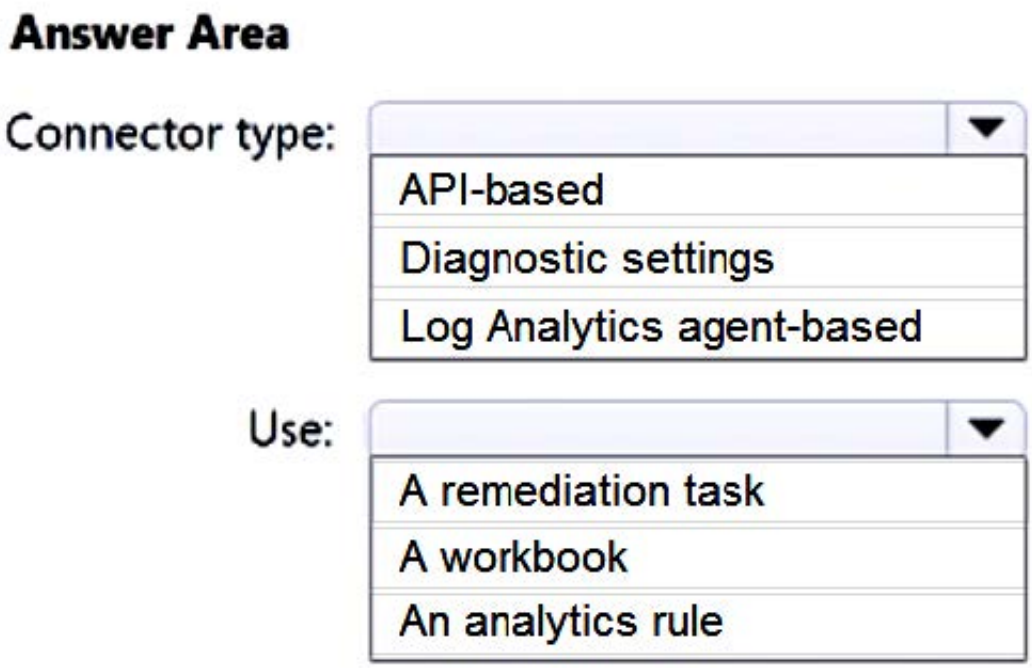
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.

You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.

Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.

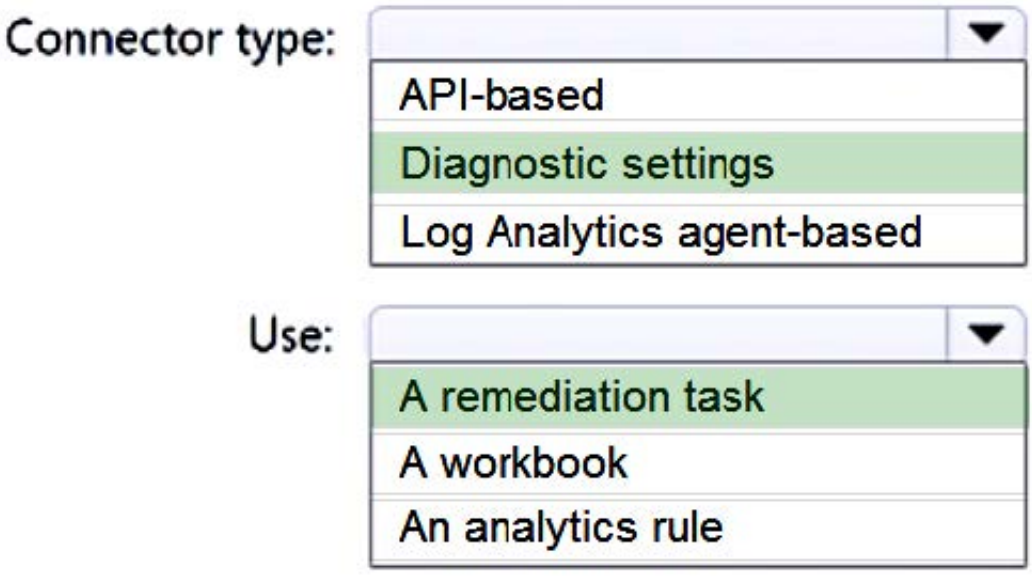
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



The policy will be applied to resources added in the future. To apply the policy on your existing resources as well, select the Remediation tab and mark the Create a remediation task check box https://learn.microsoft.com/en-us/azure/sentinel/connect-services-diagnostic-setting-based

QUESTION 15

HOTSPOT

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

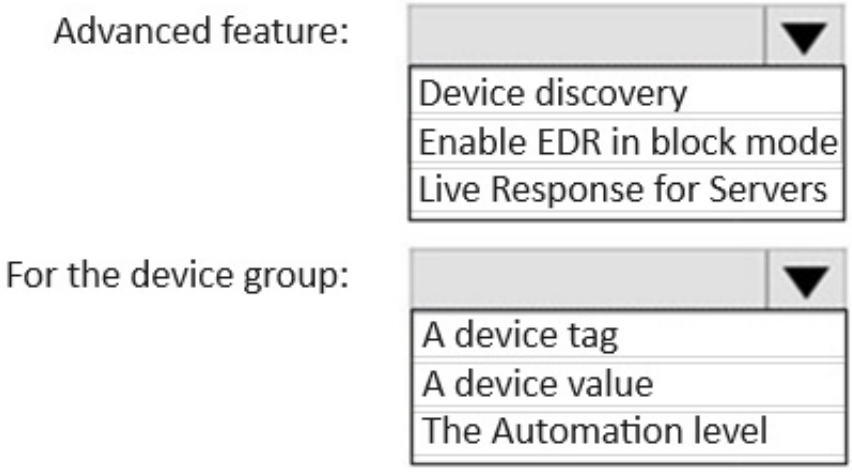
You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.

What should you configure? 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