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.leads4pass.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

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.

You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

A. From Azure Security Center, add a workflow automation.

B. On VM1, run the Get-MPThreatCatalog cmdlet.

C. On VM1 trigger a PowerShell alert.

D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Correct Answer: C

Create a suppression rule

To create a rule for a specific alert in the Azure portal:

1.

From Defender for Cloud\\'s security alerts page, select the alert you want to suppress.

2.

From the details pane, select Take action.

3.

In the Suppress similar alerts section of the Take action tab, select Create suppression rule.

4.

In the New suppression rule pane, enter the details of your new rule.

*

Entities - The resources that the rule applies to. You can specify a single resource, multiple resources, or resources that contain a partial resource ID. If you don\\'t specify any resources, the rule applies to all resources in the subscription.

*

Etc.

Incorrect:

Not D: The Get-MpThreatCatalog cmdlet gets known threats from the Windows Defender definitions catalog. The definitions catalog contains references to all known threats that Windows Defender can identify.

Example: Get a known threat from the definitions catalog

PS C:\> Get-MpThreatCatalog -ThreatID 1994

This command gets the known threat that has the ID 1994.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide

QUESTION 2

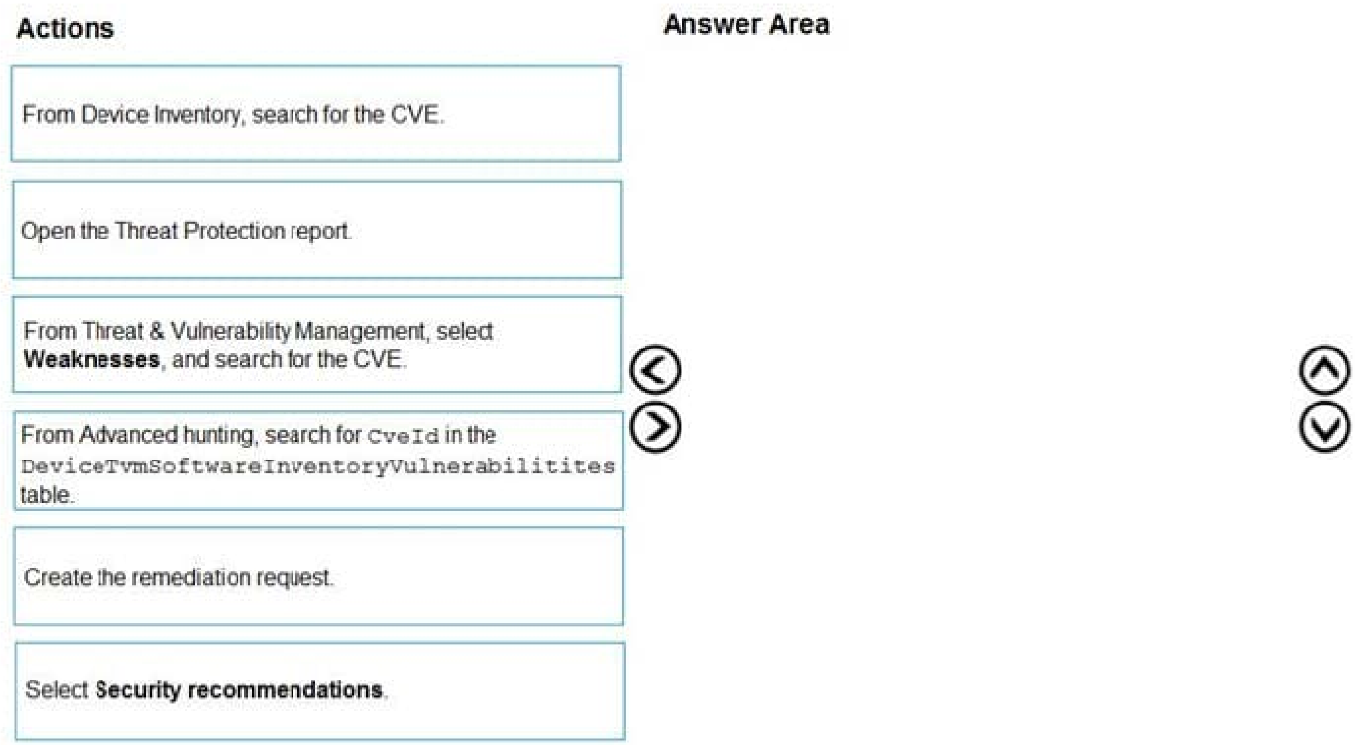
DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

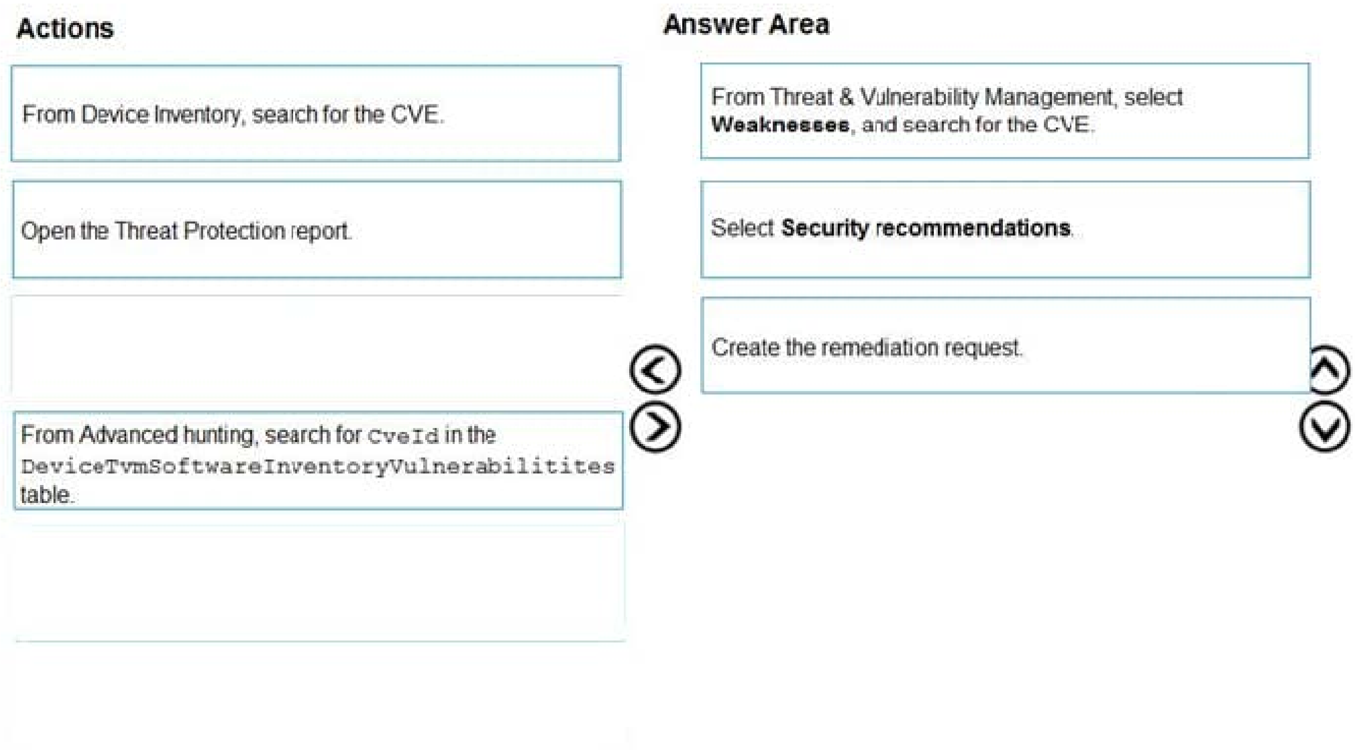
From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

Answer Area

Correct Answer:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Answer Area

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

QUESTION 3

HOTSPOT

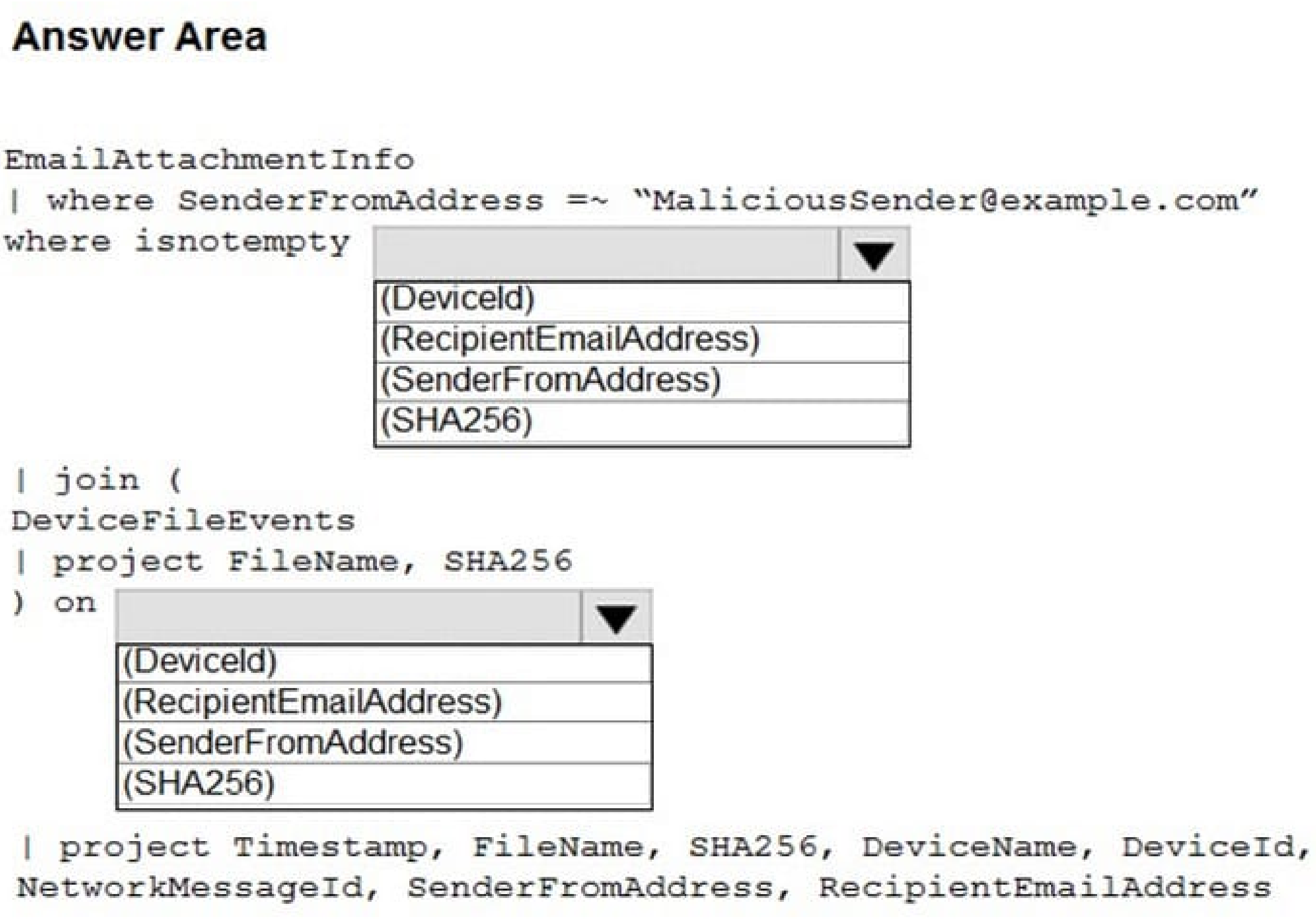
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.

You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

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

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty
```

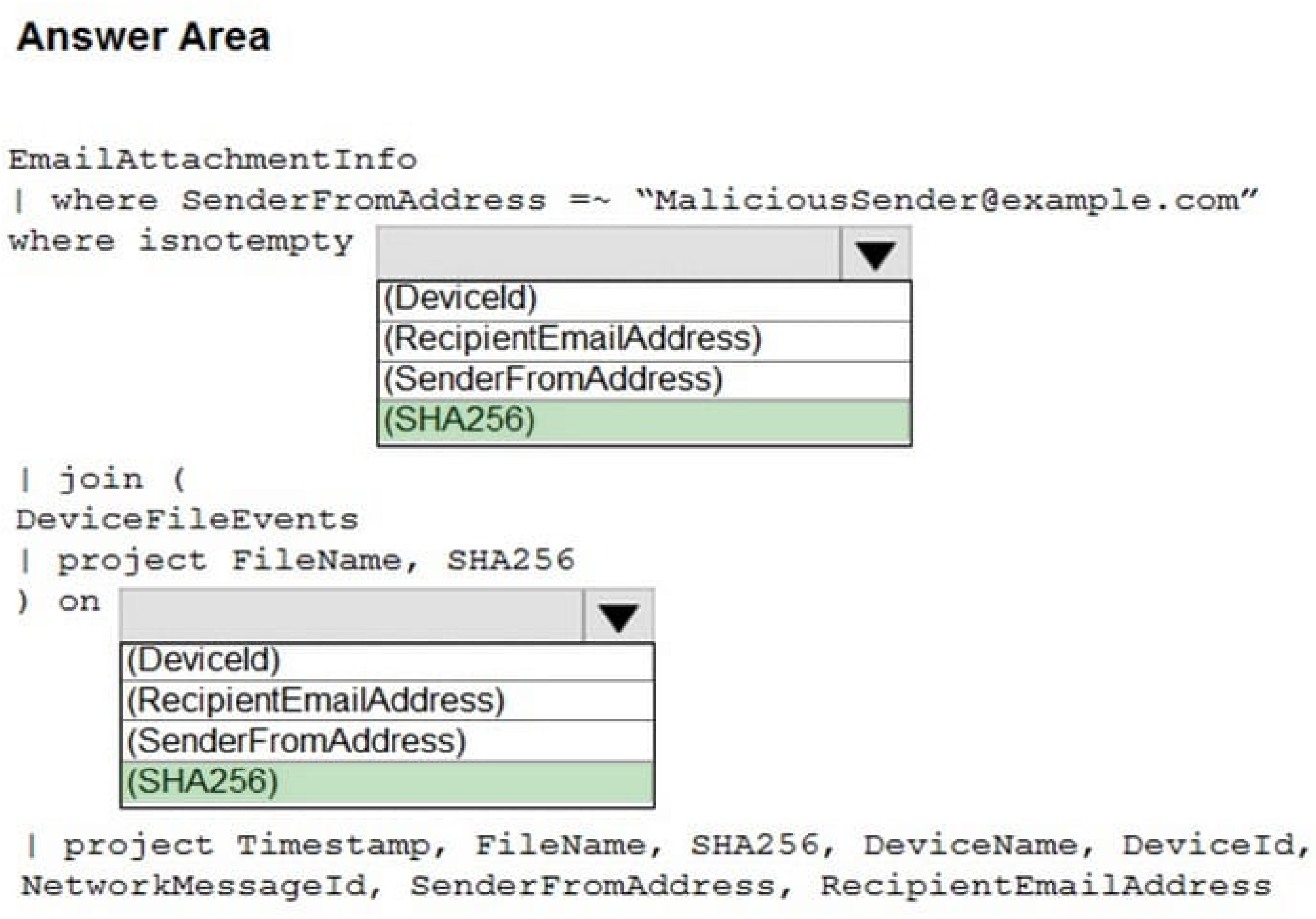
(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Correct Answer:



Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ “MaliciousSender@example.com”
where isnotempty ▼
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- [✓ (SHA256)]

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on ▼
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- [✓ (SHA256)]

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

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

QUESTION 4

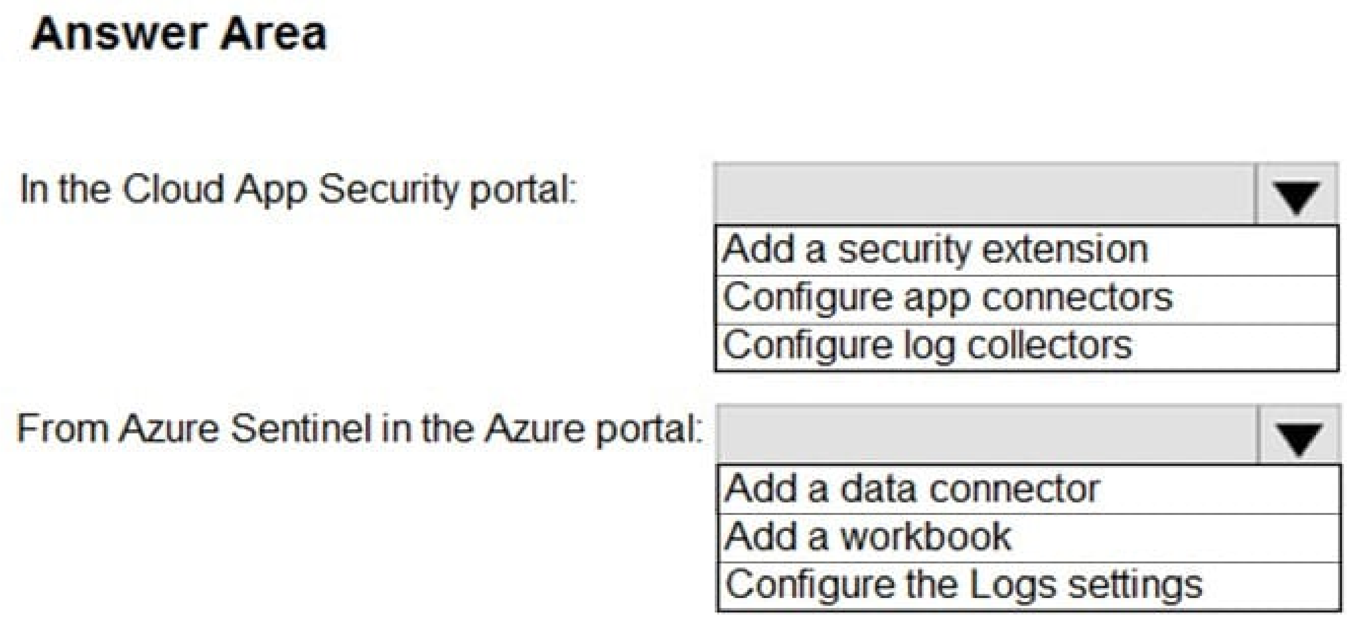
HOTSPOT

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

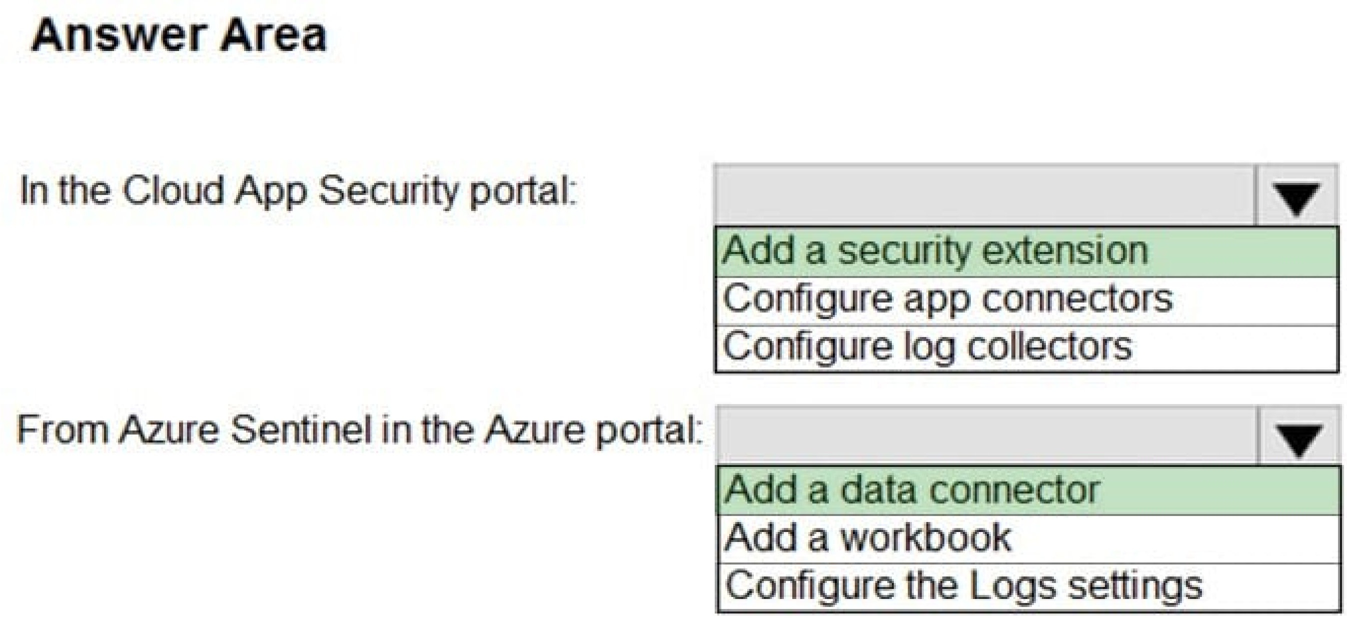
In the Cloud App Security portal: ▼

- Add a security extension
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal: ▼

- Add a data connector
- Add a workbook
- Configure the Logs settings

Correct Answer:



Answer Area

In the Cloud App Security portal: ▼

- [✓ Add a security extension]
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal: ▼

- [✓ Add a data connector]
- Add a workbook
- Configure the Logs settings

Reference: https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

QUESTION 5

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?

A. a playbook

B. a notebook

C. a livestream

D. a bookmark

Correct Answer: C

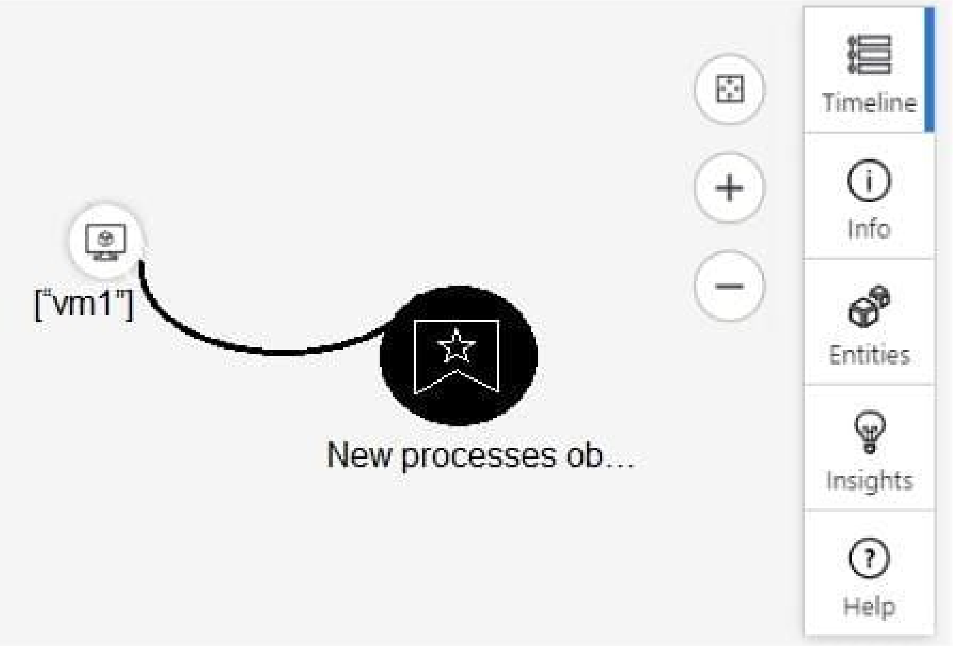
Use livestream to run a specific query constantly, presenting results as they come in.

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

QUESTION 6

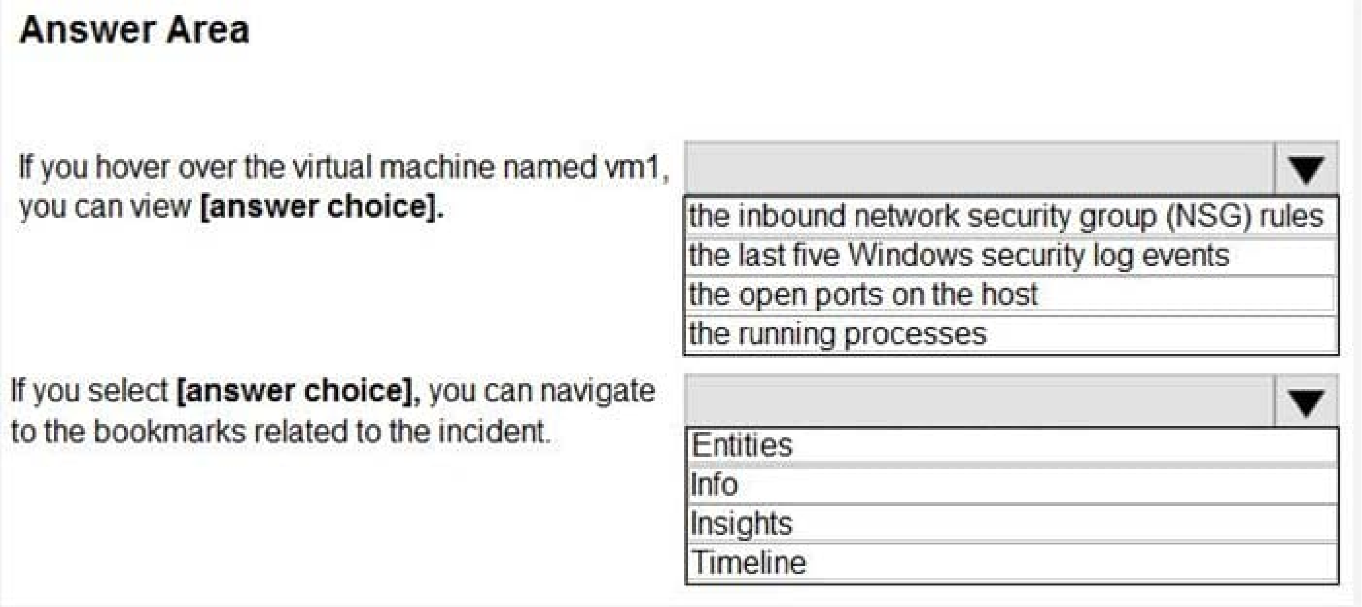
HOTSPOT

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



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:



Answer Area

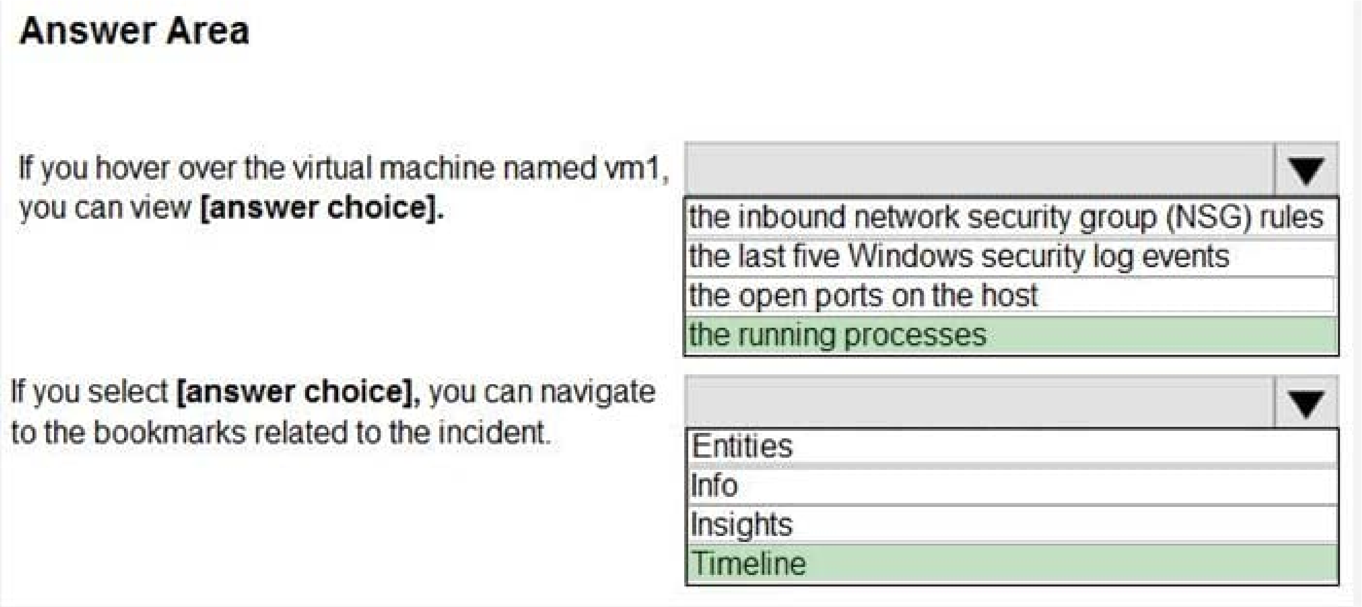
If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Correct Answer:



Answer Area

If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- [✓ the running processes]

If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

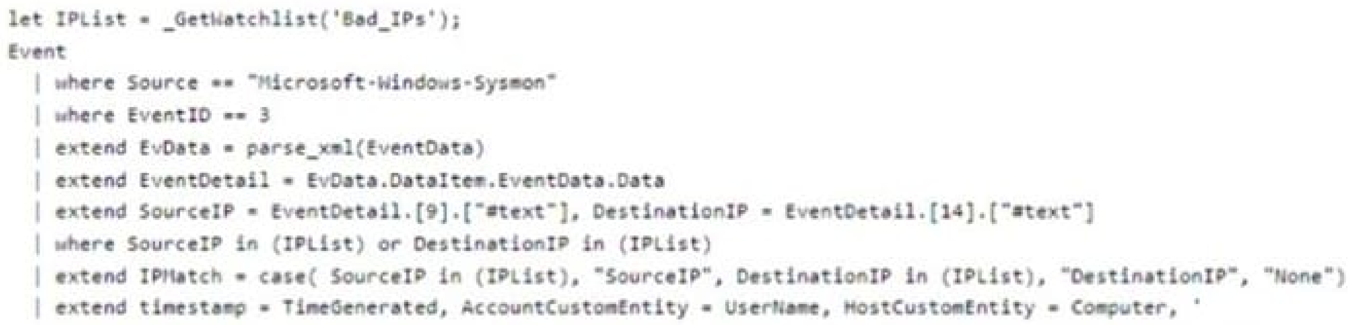
- Entities
- Info
- Insights
- [✓ Timeline]

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

QUESTION 7

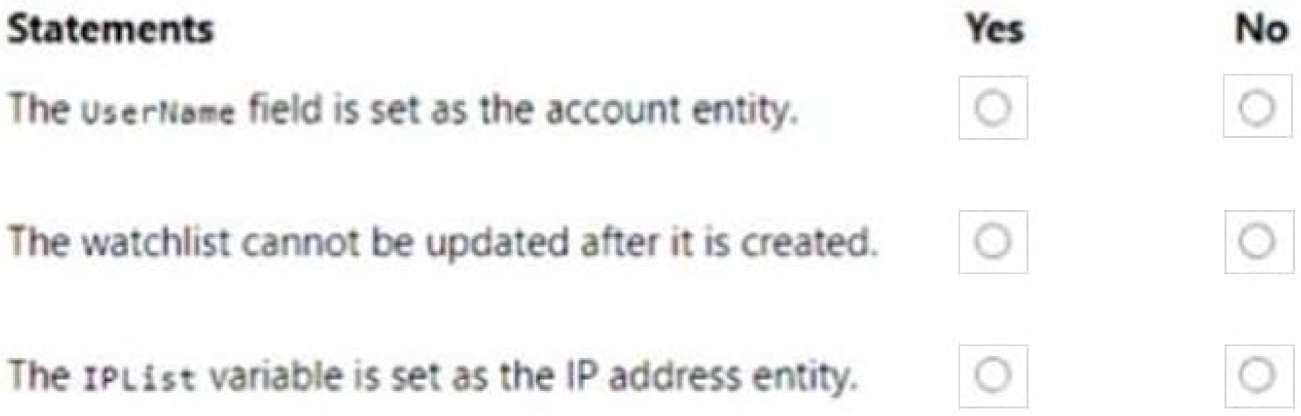
HOTSPOT

You have the following KQL query.



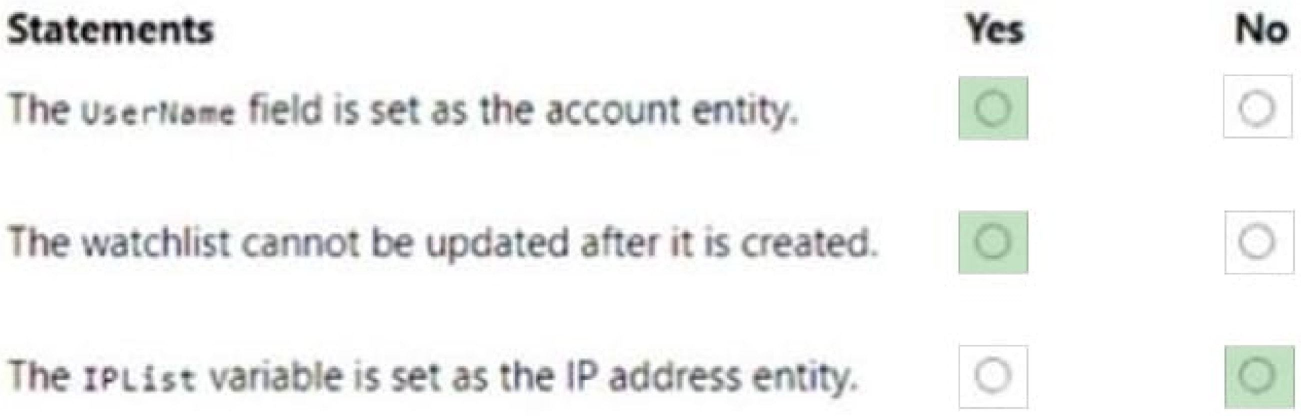
```
let IPList = _GetWatchlist('Bad_IPs');
Event
   | where Source == "Microsoft-Windows-Sysmon"
   | where EventID == 3
   | extend EvData = parse_xml(EventData)
   | extend EventDetail = EvData.DataItem.EventData.Data
   | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
   | where SourceIP in (IPList) or DestinationIP in (IPList)
   | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
   | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

Hot Area:



Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

Correct Answer:



Statements	Yes	No
The UserName field is set as the account entity.	[✓ ○]	○
The watchlist cannot be updated after it is created.	[✓ ○]	○
The IPList variable is set as the IP address entity.	○	[✓ ○]

QUESTION 8

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector.

You need to customize which details will be included when an alert is created for a specific event.

What should you do?

A. Modify the properties of the connector.

B. Create a Data Collection Rule (DCR).

C. Create a scheduled query rule.

D. Enable User and Entity Behavior Analytics (UEBA)

Correct Answer: C

https://learn.microsoft.com/en-us/azure/sentinel/customize-alert-details

QUESTION 9

You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

A. From Set rule logic, turn off suppression.

B. From Analytics rule details, configure the tactics.

C. From Set rule logic, map the entities.

D. From Analytics rule details, configure the severity.

Correct Answer: C

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

QUESTION 10

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 11

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

A. Dynamic Delivery

B. Replace

C. Block and Enable redirect

D. Monitor and Enable redirect

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

---

QUESTION 12

You need to deploy the native cloud connector to Account 1 to meet the Microsoft Defender for Cloud requirements. What should you do in Account1 first?

A. Create an AWS user for Defender for Cloud.

B. Configure AWS Security Hub.

C. Deploy the AWS Systems Manager (SSM) agent.

D. Create an Access control (IAM) role for Defender for Cloud.

Correct Answer: A

Dynamic scaled onboarding of AWS EC2 instances to Azure Arc using Ansible

Create an AWS identity

In order for Terraform to create resources in AWS, we will need to create a new AWS IAM role with appropriate permissions and configure Terraform to use it.

Scenario: Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and

does NOT have any agents installed.

Reference:

https://github.com/microsoft/azure_arc/blob/main/docs/azure_arc_jumpstart/azure_arc_servers/scaled_deployment/aws_scaled_ansible/_index.md

QUESTION 13

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

1.

Enable and disable Azure Defender.

2.

Apply security recommendations to resource.

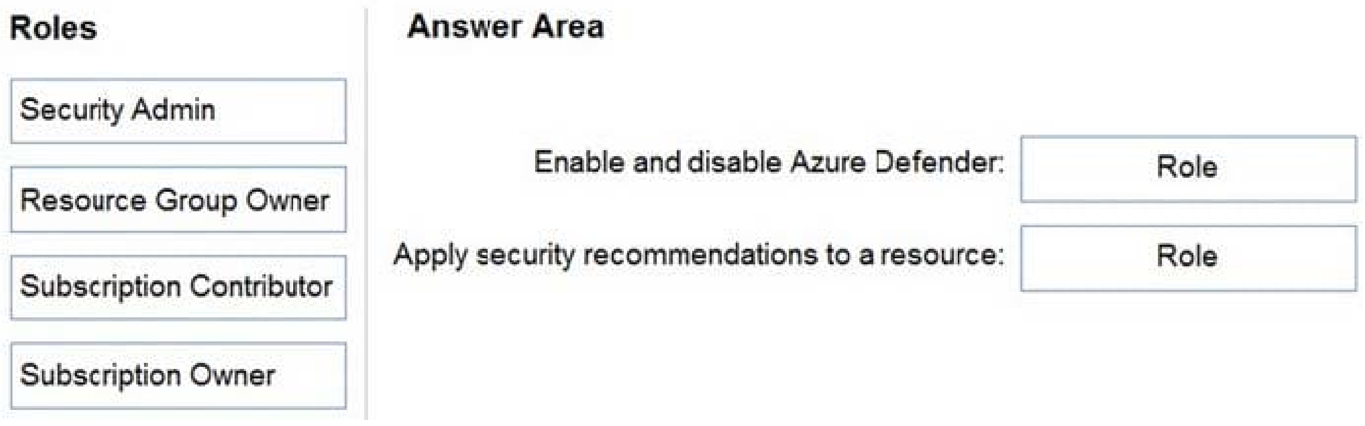
The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. 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:



Roles

Security Admin

Resource Group Owner

Subscription Contributor

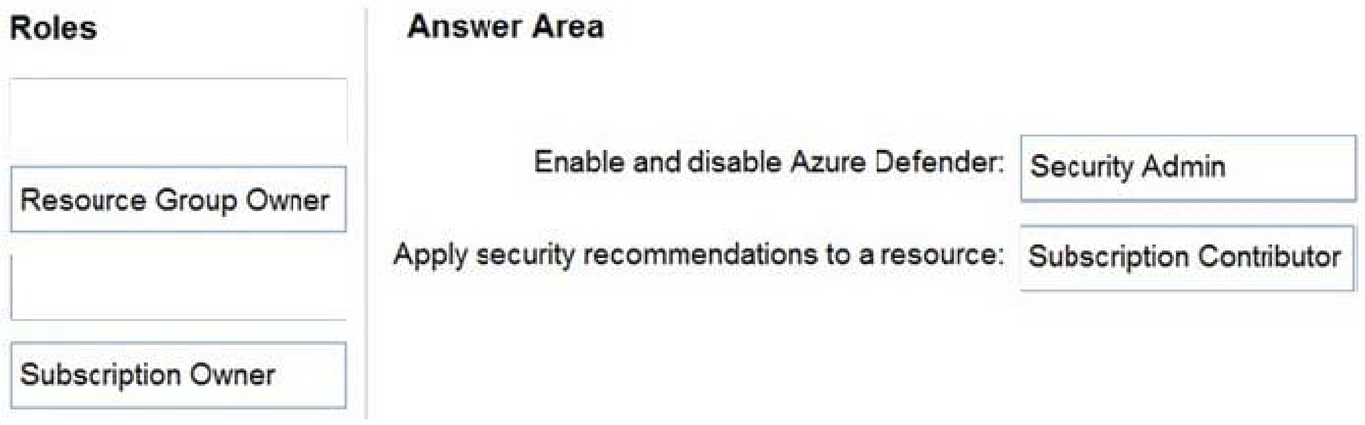
Subscription Owner

Answer Area

Enable and disable Azure Defender: Role

Apply security recommendations to a resource: Role

Correct Answer:



Roles

Resource Group Owner

Subscription Owner

Answer Area

Enable and disable Azure Defender: Security Admin

Apply security recommendations to a resource: Subscription Contributor

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

QUESTION 14

You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

A. the status update time

B. the resolution method of the source computer

C. the alert status

D. the certainty of the source computer

Correct Answer: D

Scenario: Microsoft Defender for Identity Requirements: Minimize the administrative effort required to investigate the false positive alerts.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Note: Suspected DCSync attack (replication of directory services) (external ID 2006)

Previous name: Malicious replication of directory services.

Description

Active Directory replication is the process by which changes that are made on one domain controller are synchronized with all other domain controllers. Given necessary permissions, attackers can initiate a replication request, allowing them

to retrieve the data stored in Active Directory, including password hashes.

In this detection, an alert is triggered when a replication request is initiated from a computer that isn\\'t a domain controller.

If the source computer is a domain controller, failed or low certainty resolution can prevent Defender for Identity from being able to confirm identification.

Check if the source computer is a domain controller? If the answer is yes, Close the alert as a B-TP activity.

Reference:

https://learn.microsoft.com/en-us/defender-for-identity/domain-dominance-alerts

QUESTION 15

You create a custom analytics rule to detect threats in Azure Sentinel.

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.

B. The target workspace was deleted.

C. Permissions to the data sources of the rule query were modified.

D. There are connectivity issues between the data sources and Log Analytics

Correct Answer: AD

Incorrect Answers:

B: This would cause it to fail every time, not just intermittently.

C: This would cause it to fail every time, not just intermittently.