

alerts

QUESTION 33

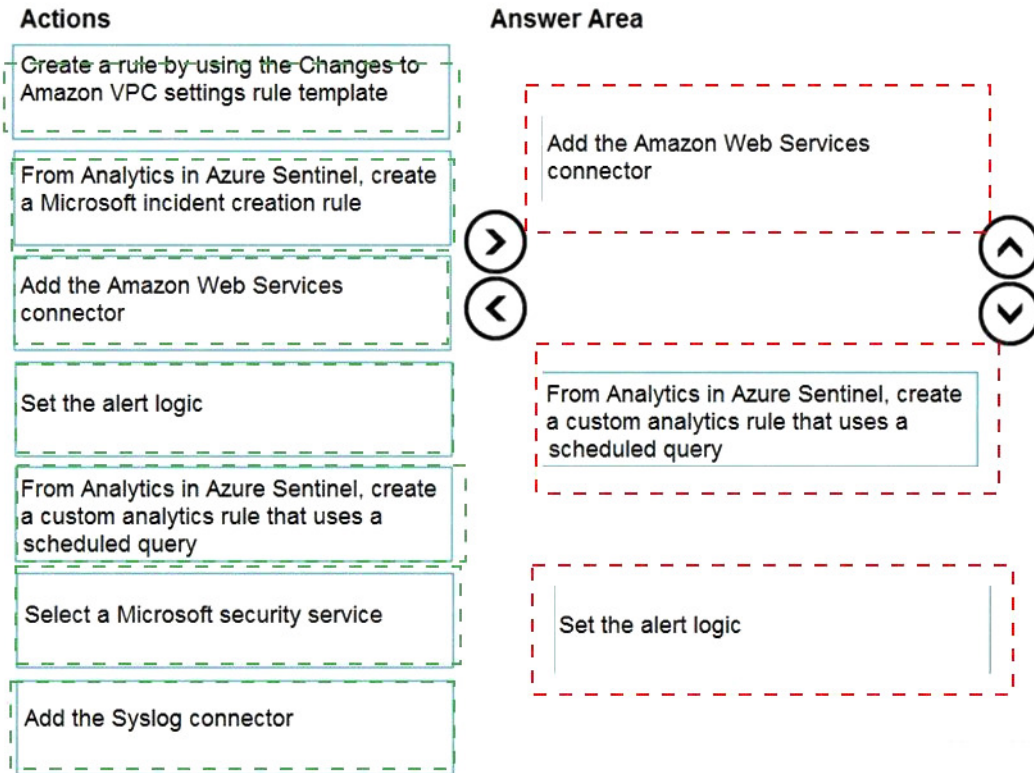
DRAG DROP

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.

Actions	Answer Area
Create a rule by using the Changes to Amazon VPC settings rule template	
From Analytics in Azure Sentinel, create a Microsoft incident creation rule	
Add the Amazon Web Services connector	
Set the alert logic	
From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query	
Select a Microsoft security service	
Add the Syslog connector	

Correct Answer:



QUESTION 34

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

QUESTION 35

HOTSPOT

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure Microsoft Defender for Endpoint:

Turn on endpoint detection and response (EDR) in block mode
Turn on Live Response
Turn off Tamper Protection

To configure the devices:

Add a network assessment job
Create a device group that contains the devices and set Automation level to Full
Create a device group that contains the devices and set Automation level to No automated response

Correct Answer:

To configure Microsoft Defender for Endpoint:

Turn on endpoint detection and response (EDR) in block mode
Turn on Live Response
Turn off Tamper Protection

To configure the devices:

Add a network assessment job
Create a device group that contains the devices and set Automation level to Full
Create a device group that contains the devices and set Automation level to No automated response

QUESTION 36

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
- B. Select Investigate files, and then filter App to Office 365.
- C. Select Investigate files, and then select New policy from search
- D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
- E. From Settings, select Information Protection, select Files, and then enable file monitoring.
- F. Select Investigate files, and then filter File Type to Document.

Correct Answer: DE

Explanation:

<https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp>

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

<https://docs.microsoft.com/en-us/cloud-app-security/azip-integration>

QUESTION 37

HOTSPOT

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.

[Home](#) > [Azure Sentinel workspaces](#) > [Azure Sentinel](#)

Analytics rule wizard – Edit existing rule

Deploy VM

[General](#) [Set rule logic](#) [Incident settings](#) [Automated response](#) [Review and create](#)

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

[View query results >](#)

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>
Host	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>
IP	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>
URL	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>
FileHash	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>

Query scheduling

Run query every *

Lookup data from the last * ⓘ

Alert threshold

Generate alert when number of query results

Event grouping

Configure how rule query results are grouped into alerts

- ☒ Group all events into a single alert
☐ Trigger an alert for each event

Suppression

Stop running query after alert is generated ⓘ

☒ On ☐ Off

Stop running query for *

[Previous](#)

[Next : Incident settings >](#)

[SC-200 Exam Dumps](#) [SC-200 PDF Dumps](#) [SC-200 VCE Dumps](#) [SC-200 Q&As](#)

<https://www.ensurepass.com/SC-200.html>

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

You do NOT define any incident settings as part of the rule definition.

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.

If a user deploys three Azure virtual machines simultaneously, how many times will you receive [answer choice] in the next five hours.

	▼
0 alerts	
1 alert	
2 alerts	
3 alerts	

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive [answer choice].

	▼
0 alerts	
1 alert	
2 alerts	
3 alerts	

Correct Answer:

If a user deploys three Azure virtual machines simultaneously, how many times will you receive [answer choice] in the next five hours.

	▼
0 alerts	
1 alert	
2 alerts	
3 alerts	

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive [answer choice].

	▼
0 alerts	
1 alert	
2 alerts	
3 alerts	

QUESTION 38

Your company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.

Which two roles should assign to the analyst? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Compliance Data Administrator in Azure Active Directory (Azure AD)
- B. the Active remediation actions role in Microsoft Defender for Endpoint
- C. the Security Administrator role in Azure Active Directory (Azure AD)
- D. the Security Reader role in Azure Active Directory (Azure AD)

Correct Answer: BD

Explanation: