SC-200$^{Q\&As}$

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

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

QUESTION 1

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to collect security event logs from the Azure virtual machines that report to workspace1.

What should you do?

A. From Security Center, enable data collection

B. In sub1, register a provider.

C. From Security Center, create a Workflow automation.

D. In workspace1, create a workbook.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

QUESTION 2

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

You need to identify all the entities affected by an incident.

Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations

B. Devices

C. Evidence and Response

D. Alerts

Correct Answer: C

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Incorrect:

*

The Investigations tab lists all the automated investigations triggered by alerts in this incident. Automated investigations will perform remediation actions or wait for analyst approval of actions, depending on how you configured your

automated investigations to run in Defender for Endpoint and Defender for Office 365.

*

Devices

The Devices tab lists all the devices related to the incident.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

QUESTION 3

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

A. extend

B. bin

C. makeset

D. workspace

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

QUESTION 4

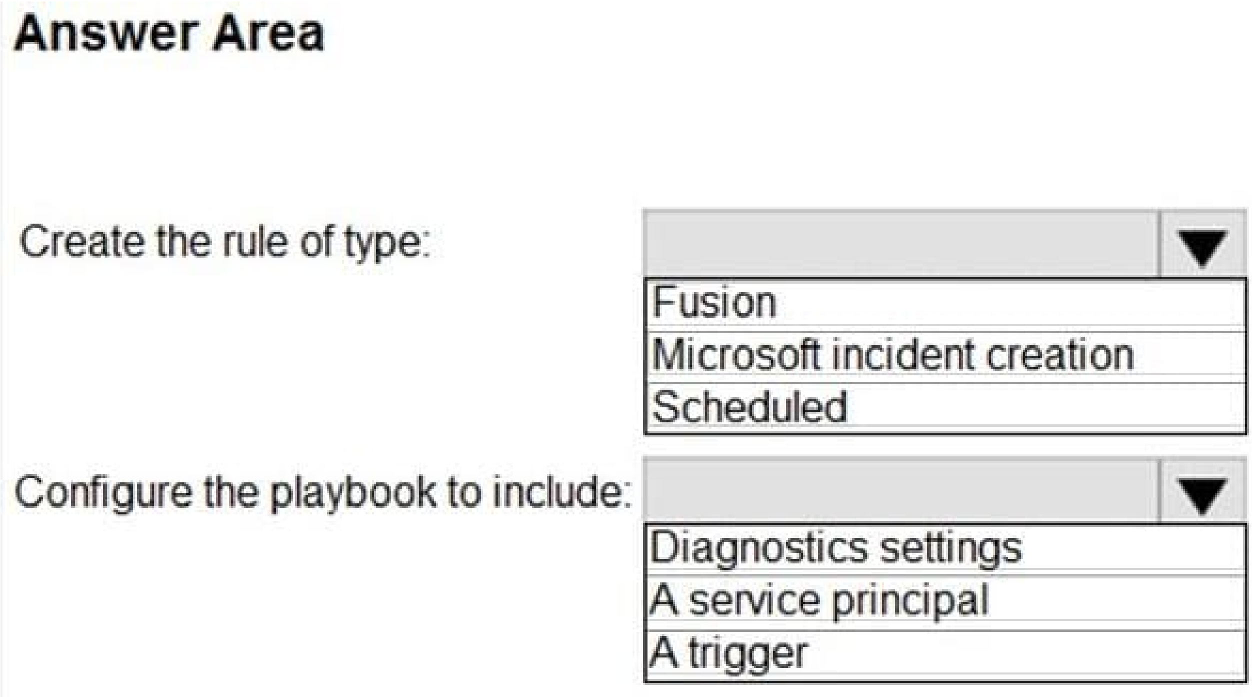
HOTSPOT

You need to create the analytics rule 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:

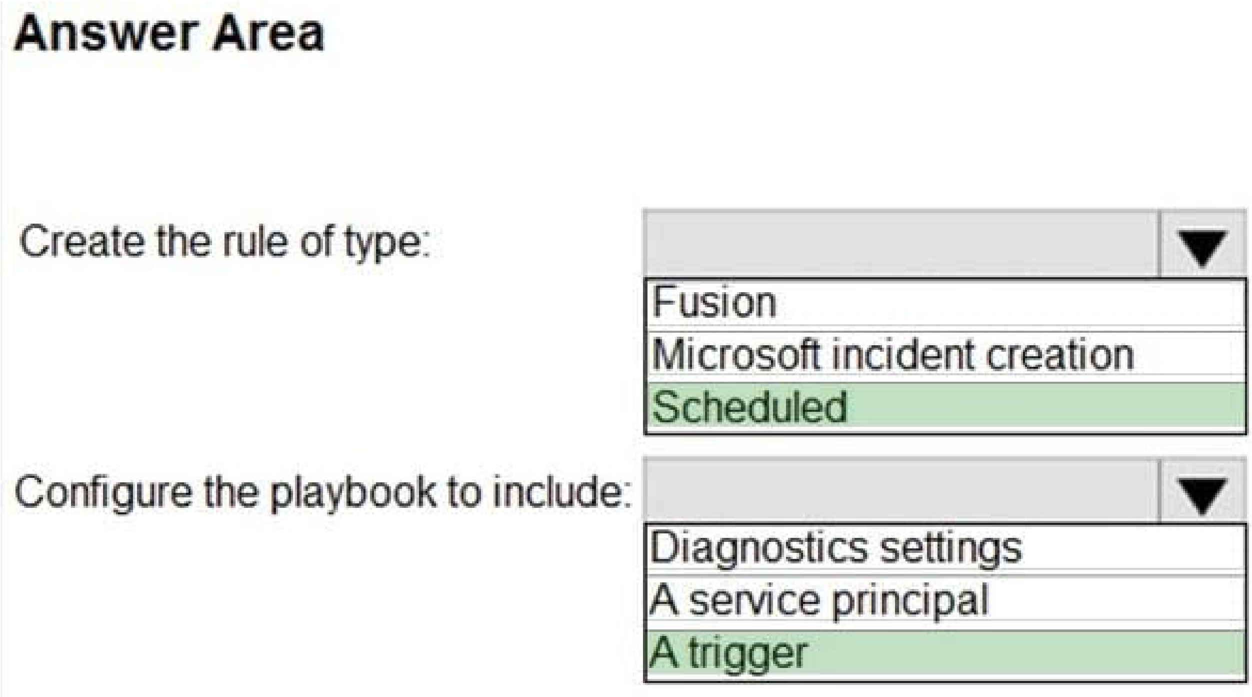


Answer Area

Create the rule of type: ▼
- Fusion
- Microsoft incident creation
- Scheduled

Configure the playbook to include: ▼
- Diagnostics settings
- A service principal
- A trigger

Correct Answer:



Answer Area

Create the rule of type: ▼
- Fusion
- Microsoft incident creation
- [✓ Scheduled]

Configure the playbook to include: ▼
- Diagnostics settings
- A service principal
- [✓ A trigger]

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 5

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC). What should you use?

A. notebooks in Azure Sentinel

B. Microsoft Cloud App Security

C. Azure Monitor

D. hunting queries in Azure Sentinel

Correct Answer: A

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