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.passapply.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

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 are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a livestream from a query.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

QUESTION 2

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 3

You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

A. a trigger

B. a connector

C. authorization

D. an API connection

Correct Answer: A

Ensure that App1 is available for use in Microsoft Sentinel automation rules.

Automation rules are made up of several components:

Triggers that define what kind of incident event will cause the rule to run, subject to...

Conditions that will determine the exact circumstances under which the rule will run and perform...

Actions to change the incident in some way or call a playbook.

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

QUESTION 4

You need to investigate a potential attack deploying a new ransomware strain.

You will perform automated actions on a group of highly valuable machines containing sensitive information.

There are three custom device groups.

You are required to temporarily group the machines to perform actions on the devices.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a tag to the device group.

B. Create a new device group that has a rank of 1.

C. Create a new device group that has a rank of 4.

D. Create a new admin role.

E. Add a tag to the machines.

F. Add the device users to the admin role.

Correct Answer: ABE

Reference: https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/

QUESTION 5

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