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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1 contains 20 virtual machines that run Windows Server 2019. You need to configure just-in-time (JIT) access for the virtual machines in RG1. The solution must meet the following requirements:

1.

Limit the maximum request time to two hours.

2.

Limit protocols access to Remote Desktop Protocol (RDP) only.

3.

Minimize administrative effort. What should you use?

A. Azure AD Privileged Identity Management (PIM)

B. Azure Policy

C. Azure Bastion

D. Azure Front Door

Correct Answer: C

You can combine Azure Bastion with the JIT VM access feature of Microsoft Defender for Cloud. JIT provides just-in-time network-based access to VMs by locking down your VMs at the network level and blocking all unnecessary inbound traffic to specific management ports, like RDP or SSH. To be able to do this, it adds a deny rule to the Azure network security group (NSG), which protects the VM network interface or the subnet it belongs to.

When a user then requests access to the VM, the service adds a temporary allow rule to the NSG. Because the allow rule has a higher priority than the deny rule, the user can connect to the VM. The user can also only connect for a limited amount of time, with a maximum of 24 hours. This time limit is specified when JIT is configured for a specific VM or VMs.

Reference: https://wmatthyssen.com/2022/11/28/azure-bastion-combine-jit-with-azure-bastion

QUESTION 2

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

---

QUESTION 3

You have a Microsoft Sentinel workspace named Workspace1.

You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser.

What should you create in Workspace1?

A. a watch list

B. an analytic rule

C. a hunting query

D. a workbook

Correct Answer: A

To support excluding built-in source-specific parsers, ASIM uses a watchlist. Deploy the watchlist to your Microsoft Sentinel workspace from the Microsoft Sentinel GitHub repository. Reference: https://learn.microsoft.com/en-us/azure/sentinel/normalization-manage-parsers

---

QUESTION 4

HOTSPOT

You have an Azure subscription that uses Azure Defender.

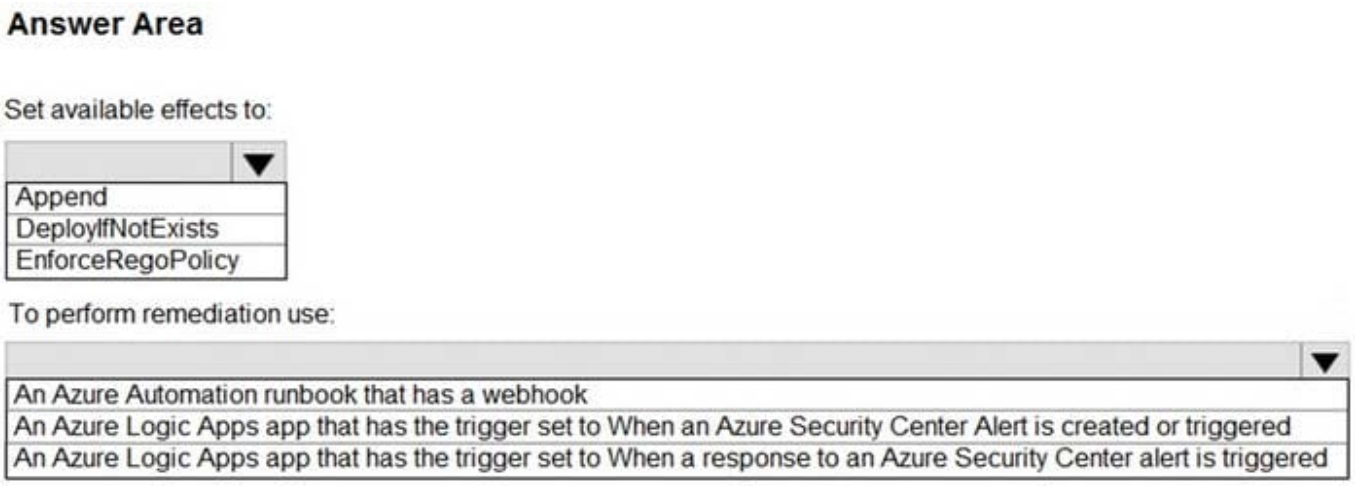
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

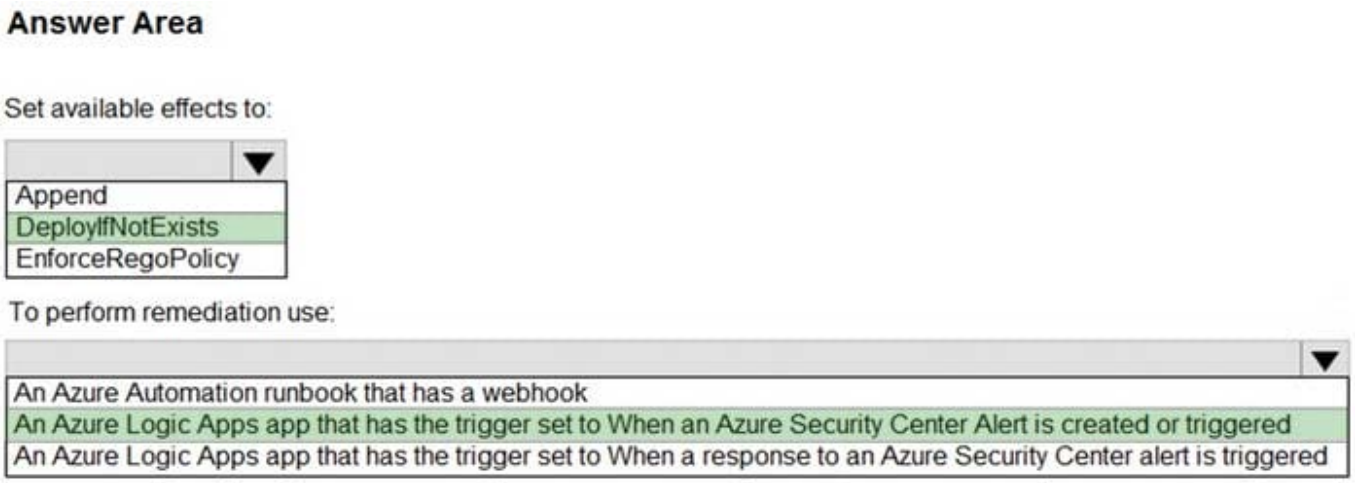
What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

QUESTION 5

A user wants to sign in from a location which has never been used by the other users in your organization. Which anomaly detection policy will you use if you need to receive a security alert ?

A. Activity from infrequent country

B. Activity from anonymous IP addresses

C. Impossible travel

D. Malware detection

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

SC-200 VCE Dumps SC-200 Practice Test SC-200 Study Guide