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 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 2

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 3

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

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

QUESTION 4

You create an Azure subscription.

You enable Azure Defender for the subscription.

You need to use Azure Defender to protect on-premises computers.

What should you do on the on-premises computers?

A. Install the Log Analytics agent.

B. Install the Dependency agent.

C. Configure the Hybrid Runbook Worker role.

D. Install the Connected Machine agent.

Correct Answer: A

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats. Data is collected using:

1.

The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.

2.

Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

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

QUESTION 5

Your company deploys the following services:

1.

Microsoft Defender for Identity

2.

Microsoft Defender for Endpoint

3.

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

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