



Free Questions for SC-200 by dumpshq

Shared by Fischer on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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 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?

Options:

A- Yes

B- No

Answer:

B

Explanation:

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

Question 2

Question Type: MultipleChoice

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 have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You manually install the Log Analytics agent on the virtual machines.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc>

Question 3

Question Type: MultipleChoice

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 have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc>

Question 4

Question Type: MultipleChoice

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 suppress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

Options:

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.

Answer:

C

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide>

Question 5

Question Type: MultipleChoice

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

Options:

- A- Create an Azure Sentinel workspace that has a Security Events connector.
- B- Configure the Diagnostics settings in Azure AD to stream to an event hub.
- C- Create an Azure Sentinel workspace that has an Azure Active Directory connector.
- D- Configure the Diagnostics settings in Azure AD to archive to a storage account.

Answer:

B

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

Question 6

Question Type: MultipleChoice

You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.

You need to mitigate the following device threats:

Microsoft Excel macros that download scripts from untrusted websites

Users that open executable attachments in Microsoft Outlook

Outlook rules and forms exploits

What should you use?

Options:

A- Microsoft Defender Antivirus

B- attack surface reduction rules in Microsoft Defender for Endpoint

C- Windows Defender Firewall

D- adaptive application control in Azure Defender

Answer:

B

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide>

To Get Premium Files for SC-200 Visit

<https://www.p2pexams.com/products/sc-200>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/sc-200>

