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

---

QUESTION 2

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 3

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

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

NOTE: Each correct selection is worth one point.

A. Create a livestream

B. Add a data connector

C. Create an analytics rule

D. Create a hunting query.

E. Create a bookmark.

Correct Answer: BD

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

QUESTION 4

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema.

You need to make the 200 parses available in Workspace1. The solution must minimize administrative effort.

What should you do first?

A. Copy the parsers to the Azure Monitor Logs page.

B. Create a JSON file based on the DNS template.

C. Create an XML file based on the DNS template.

D. Create a YAML file based on the DNS template.

Correct Answer: D

Deploy parsers

Deploy parsers manually by copying them to the Azure Monitor Log page and saving the query as a function. This

method is useful for testing.

To deploy a large number of parsers, we recommend using parser ARM templates, as follows:

Create a YAML file based on the relevant template for each schema and include your query in it. Start with the YAML template relevant for your schema and parser type, filtering or parameter-less.

Use the ASIM Yaml to ARM template converter to convert your YAML file to an ARM template.

If deploying an update, delete older versions of the functions using the portal or the function delete PowerShell tool.

Deploy your template using the Azure portal or PowerShell.

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/normalization-develop-parsers

QUESTION 5

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days.

What should you use?

A. the Azure Active Directory Provisioning Analysis workbook

B. the Overview settings of Insider risk management

C. the Modifications of sensitive groups report in Microsoft Defender for Identity

D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Correct Answer: C

Track changes to sensitive groups with Advanced Hunting in Microsoft 365 Defender.

In my role working with Defender for Identity (MDI) customers, I\\'m often asked if MDI can help them answer questions about activities taking place within the environment. MDI does have a lot of information around the activities taking place in

Active Directory and now combined with the power of Advanced Hunting in Microsoft 365 Defender, we can help customers answer some these questions with ease and efficiency.

1.

MDI tracks the changes made to Active Directory group memberships. These changes are recorded by MDI as an activity and are available in the Microsoft 365 Defender Advanced Hunting, IdentityDirectoryEvents. MDI records these changes from two different sources:

2.

Tracking changes made to an entity by the Active Directory Update Sequence Number (USN). In the case of a group, MDI can see who has been added or removed from a group, but we don\\'t see the actor who made the change or which

domain controller the change was made on.

Tracking changes to a group, including who performed the action. MDI requires specific Windows events to be recorded on the domain controller.

Reference: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/track-changes-to-sensitive-groups-with-advanced-hunting-in/ba-p/3275198