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.geekcert.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 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 2

The custom analytics rule which can detect threats in Azure Sentinel stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED. What is the problem?

A. The number of alerts exceeded 10,000 within two minutes.

B. There are connectivity issues between the data sources and Log Analytics.

C. The rule query takes too long to run and times out.

D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 3

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

A. Azure Sentinel Responder

B. Logic App Contributor

C. Azure Sentinel Contributor

D. Azure Sentinel Reader

Correct Answer: A

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

QUESTION 4

HOTSPOT

You need to create a query for a workbook. The query must meet the following requirements:

1.

List all incidents by incident number.

2.

Only include the most recent log for each incident.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
SecurityIncident
| [project / sort / summarize] [arg_max / limit / top] (LasModifiedTime,*) by IncidentNumber
```

Correct Answer:

Answer Area

```
SecurityIncident
| [project / sort / summarize] [arg_max / limit / top] (LasModifiedTime,*) by IncidentNumber
```

Reference: https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

QUESTION 5

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription

B. the Contributor for the subscription

C. the Contributor role for RG1

D. the Owner role for RG1

Correct Answer: C