SC-900 Q&As

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sc-900.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

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point

Hot Area:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	○	○

Correct Answer:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	●	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	●
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	●	○

Box 1: Yes

From Microsoft Defender for cloud you can enable Microsoft Defender for Storage to get alerted about suspicious

activities related to your storage resources.

Note: Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your storage accounts.

Defender for Storage continually analyzes the telemetry stream generated by the Azure Blob Storage and Azure Files services. When potentially malicious activities are detected, security alerts are generated. These alerts are displayed in

Microsoft Defender for Cloud, together with the details of the suspicious activity along with the relevant investigation steps, remediation actions, and security recommendations.

Box 2: No Box 3: Yes

Microsoft Defender for Cloud is a solution for cloud security posture management (CSPM) and cloud workload protection (CWP) that finds weak spots across your cloud configuration, helps strengthen the overall security posture of your environment, and can protect workloads across multicloud and hybrid environments from evolving threats.

Microsoft Defender for Servers is one of the plans provided by Microsoft Defender for Cloud\\'s enhanced security features. Defender for Servers protects your Windows and Linux machines in Azure, AWS, GCP, and on-premises.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction

QUESTION 2

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Correct Answer:

Reference: https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

QUESTION 3

Which Microsoft 365 compliance feature can you use to encrypt content automatically based on specific conditions?

A. Content Search

B. sensitivity labels

C. retention policies

D. eDiscovery

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

QUESTION 4

You have an Azure subscription that contains a Log Analytics workspace.

You need to onboard Microsoft Sentinel.

What should you do first?

A. Create a hunting query.

B. Correlate alerts into incidents.

C. Connect to your security sources.

D. Create a custom detection rule.

Correct Answer: C

https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources After you onboard Microsoft Sentinel into your workspace, use data connectors to start ingesting your data into Microsoft Sentinel. Microsoft Sentinel comes with many out of the box connectors for Microsoft services, which integrate in real time. For example, the Microsoft 365 Defender connector is a service-to-service connector that integrates data from Office 365, Azure Active Directory (Azure AD), Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

QUESTION 5

Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a network interface

B. an Azure App Service web app

C. a virtual network

D. a virtual network subnet

E. E. a resource group

Correct Answer: AD

Association of network security groups

You can associate a network security group with virtual machines, NICs, and subnets, depending on the deployment model you use.

Reference:

https://aviatrix.com/learn-center/cloud-security/create-network-security-groups-in-azure/