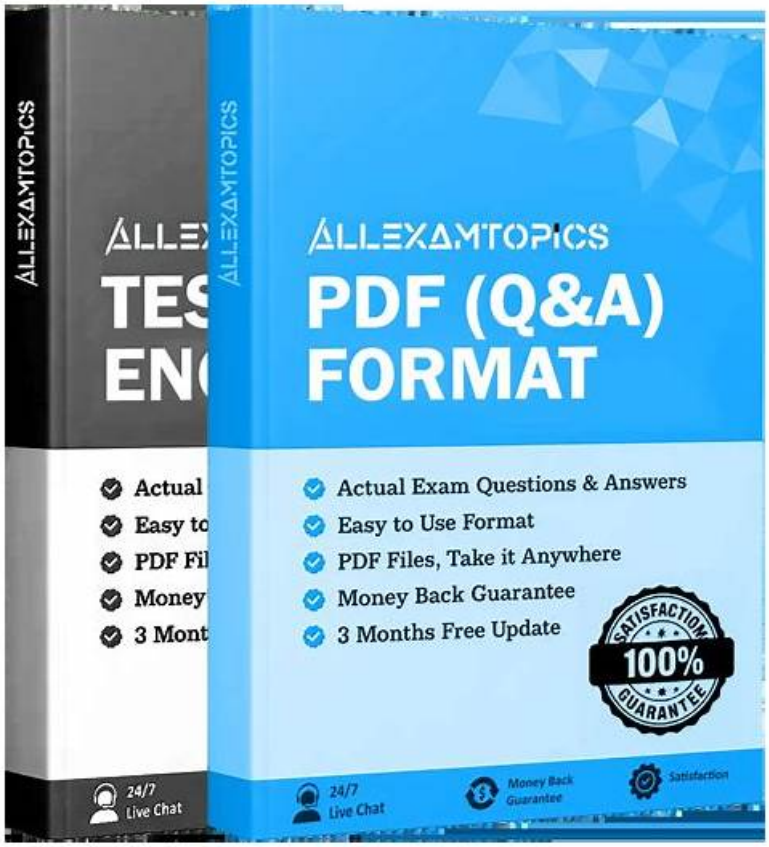
SC-500 Questions - Highly Recommended By Professionals



The Implementing End-to-End Security Controls for Cloud and AI Workloads can advance your professional standing. Passing the Microsoft SC-500 exam is the requirement to become Microsoft Professionals and to get your name included. Practicing with Microsoft SC-500 Dumps is considered the best strategy to test the exam readiness. After passing the SC-500 exam you will become a valuable asset for the company you work for or want to work. You don't need to sacrifice your job hours or travel to distant training institutes for exam preparation when you have Microsoft SC-500 Dumps for instant success. These SC-500 dumps questions with authentic answers are compiled by Microsoft professionals and follow the actual exam's questioning style.

Microsoft SC-500 Exam Syllabus Topics:

Section	Weight	Objectives
Manage and monitor security posture	20-25%	- Implement Microsoft Security Copilot configuration - Manage security posture using Microsoft Defender for Cloud - Implement activity and event collection in Microsoft Sentinel
Manage identity, access, and governance	20-25%	- Secure access to resources using Microsoft Entra ID - Implement governance with Azure Policy and Defender for Cloud - Secure secrets and keys using Azure Key Vault
Secure compute	20-25%	- Implement security for AI workloads - Implement security for application platform services - Implement security for servers and virtual machines (VMs)
Secure storage, databases, and networking	25-30%	- Implement security for databases - Implement security for storage accounts - Implement security for Azure network services

>> Examinations SC-500 Actual Questions <<

Free PDF SC-500 - Implementing End-to-End Security Controls for Cloud and AI Workloads Updated Examinations Actual Questions

There are more opportunities for possessing with a certification, and our SC-500 study tool is the greatest resource to get a leg up on your competition, and stage yourself for promotion. When it comes to our time-tested SC-500 latest practice dumps, for one thing, we have a professional team contains a lot of experts who have devoted themselves to the research and development of our SC-500 Exam Guide, thus we feel confident enough under the intensely competitive market. For another thing, conforming to the real exam our SC-500 study tool has the ability to catch the core knowledge. So our customers can pass the exam with ease.

Microsoft Implementing End-to-End Security Controls for Cloud and AI Workloads Sample Questions (Q105-Q110):

NEW QUESTION # 105
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft Sentinel workspace.
You have a multi-tier Security Operations Center (SOC) team.
You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.
Solution: You create a hunting query.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:
A hunting query is used to investigate threats and identify suspicious activity; it does not automatically assign newly created incidents or flag them for triage. An automation rule triggered when an incident is created is required to assign incidents to the Tier 1 analysts group and apply a triage tag or task automatically.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules?tabs=defender-portal%2Conboarded

NEW QUESTION # 106
You have an Azure subscription named Sub1 that contains multiple virtual machines.
You have a Microsoft 365 E5 subscription that contains devices onboarded to Microsoft Defender for Endpoint.
You have an on-premises datacenter that contains multiple servers.
You plan to onboard all existing and future on-premises servers to Azure Arc.
You need to ensure that the Azure Arc-enabled servers are protected by using the same security features as the Microsoft 365 devices immediately after the servers are onboarded. The solution must minimize administrative effort.
What should you do?

- A. Onboard each server to Microsoft Defender for Endpoint by using a local installation script.
- B. Onboard each server to Microsoft Defender for Endpoint by using Group Policy.
- C. Configure an Azure Policy assignment.
- D. For Sub1, enable the Microsoft Defender for Servers plan in Microsoft Defender for Cloud.

Answer: D

Explanation:
When on-premises servers are onboarded to Azure Arc, Microsoft Defender for Servers can extend Microsoft Defender for Endpoint integration and server protection policies to them centrally. Enabling the Defender for Servers plan in the subscription minimizes manual effort and applies protection as Arc resources come under Defender for Cloud. Local scripts or Group Policy deployments protect current servers only and are weaker for future automatic onboarding. For SC-500, compute controls are evaluated by workload type: VM, Arc server, AKS, container registry, container group, Functions, Logic Apps, App Service, and AI agent runtime.

The right answer uses the Microsoft control that is native to that workload. Broad Azure roles or unrelated monitoring services would either overgrant access or fail to enforce the required security state. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > onboard servers to Defender for Servers; Microsoft Learn > Defender for Servers and Azure Arc integration.

NEW QUESTION # 107
You have an Azure Functions app named App1 that uses an HTTP trigger, runs on an Elastic Premium plan, and uses virtual network integration.
A partner application sends requests to App1 from a public IP address of xxx.xxx.xxx.xx.
You need to ensure that the requests are accepted from only xxx.xxx.xxx.xx.
What should you do?

- A. Configure an inbound access restriction on App1.
- B. Create a private endpoint for App1 and disable public network access.
- C. Apply a network security group (NSG) to a dedicated subnet for virtual network integration.
- D. Deploy an Azure NAT Gateway.
- E. Deploy an Azure Bastion host.

Answer: A

Explanation:
To restrict access to your Azure Functions app so that it only accepts requests from the specific public IP address xxx.xxx.xxx.xx, you should configure Access Restrictions (IP filtering) on the Azure Functions app.
Because your app runs on an Elastic Premium plan, it includes native support for networking features like access restrictions. This will block all other public traffic at the Azure App Service platform layer before it even reaches your function code.
Reference:
https://learn.microsoft.com/en-us/azure/azure-functions/functions-networking-options

NEW QUESTION # 108
You have a Microsoft Sentinel workspace named Workspace1
You have 100 on-premises servers that run Linux and have the Azure Monitor Agent installed.
You need to collect Syslog events from the Linux servers. The solution must meet the following requirements:
*Ensure that filtering occurs before data is written to Workspace1
*Reduce ingestion costs by excluding low value Syslog messages.
What should you include in the solution?

- A. An analytics rule
- B. A table-level filter and split transformation
- C. An Advanced Security Information Model (ASIM) parser
- D. A data collection rule (DCR)

Answer: D

Explanation:
Filtering must happen before data is written to the Log Analytics workspace. With Azure Monitor Agent, Syslog collection is governed by data collection rules, and DCR transformations or filtering can reduce ingestion before records reach the workspace. An ASIM parser normalizes queried data after ingestion, an analytics rule detects conditions after data exists, and a table-level transformation is not the primary collection control for Linux Syslog from AMA in this scenario. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Syslog event collection; Microsoft Learn > data collection rules for Azure Monitor Agent.
Topic 1, Contoso Ltd.Case Study: Contoso, Ltd.
Company Background
Contoso, Ltd. is a financial analytics company that is modernizing its cloud security architecture in Microsoft Azure. Contoso uses Azure Kubernetes Service, Azure Functions, Azure SQL Database, Azure Storage, Microsoft Defender for Cloud, Microsoft Entra

Privileged Identity Management, and Azure Arc to secure production workloads and AI-based services.
Contoso has one Azure subscription named Sub1 that is linked to a Microsoft Entra tenant named contoso.
com .
Existing Azure Environment
Subscription and Resource Groups
Sub1 contains the following resource groups:
Resource Group
Purpose
RG-App
Hosts production application workloads
RG-Data
Hosts storage and database services
RG-Security
Hosts monitoring and security resources
RG-AI
Hosts AI and agent-related workloads
Compute Resources
Contoso has the following compute resources:
Resource
Type
Description
AKS1
Azure Kubernetes Service cluster
Hosts production containerized applications
ACR1
Azure Container Registry
Stores container images used by AKS1
Fa1
Azure Function App
Processes production AI transaction events
Fa2
Azure Function App
Runs test and diagnostic jobs only
Fa3
Azure Function App
Processes production security automation events
Server1
On-premises server
Hosts a legacy security processing workload
AKS1 uses a managed identity. A separate user-assigned managed identity named ID1 is used by the deployment automation process.
Data Resources
Contoso has the following data resources:
Resource
Type
Description
SQLServer1
Azure SQL logical server
Hosts production SQL databases
SQLdb1
Azure SQL Database
Stores sensitive application data
storage2
Azure Storage account
Stores AI output files and security processing artifacts
Current Security Configuration
Microsoft Defender for Cloud is enabled for Sub1. Defender Cloud Security Posture Management is also enabled.
Contoso has not yet enabled a Defender workload protection plan for AKS1.
Server1 is not currently connected to Azure. The security team wants Server1 to be visible in Azure for monitoring, compliance, and security operations.
Users and Administrators

The Microsoft Entra tenant contains the following users:
User
Current Role / Responsibility
User1
AI engineering user who requests privileged access when required
Admin1
Security administrator for Sub1 and approved Defender for Cloud delegate Admin2 General application administrator Admin3 Privileged Role Administrator for Microsoft Entra roles Admin4 Helpdesk administrator Privileged Identity Management Configuration Contoso uses Microsoft Entra Privileged Identity Management.
The following PIM role settings are configured:
Role
Approval Required
Eligible Approvers
Maximum Active Duration
AI Administrator
Yes
Admin1 and Admin3 only
1 day
Agent ID Developer
Yes
Admin1 only
2 days
Admin3 has permission to manage eligible and active assignments for Microsoft Entra roles.
Admin2 is not configured as an approver for the AI Administrator role.
Planned Changes
Contoso plans to implement the following changes:
* Configure AKS1 so that it can pull images from ACR1 without granting unnecessary permissions.
* Configure ID1 so that the deployment automation process can modify Azure resources required by the application deployment.
* Configure SQLdb1 so that access is controlled by Microsoft Entra authentication and Conditional Access.
* Configure storage2 so that selected blobs can use a separate encryption boundary without changing encryption for the entire storage account.
* Implement the production Function App security changes only for Function Apps that process production workload data.
* Enable the correct Microsoft Defender for Cloud plan to protect applications running on AKS1.
* Delegate the Defender for Cloud planned change to the least-privileged administrator.
* Configure Server1 so that it can be monitored and managed through Azure security tooling.
Technical Requirements
Contoso has the following technical requirements:
AKS and Container Registry
* AKS1 must pull container images from ACR1.
* AKS1 must receive only the minimum role required to pull images.
* The managed identity ID1 must be able to perform deployment automation tasks that modify Azure resources.
* Permissions must follow the principle of least privilege.
Azure SQL Database
* SQLdb1 must support Microsoft Entra-based authentication.
* Access to SQLdb1 must be controlled by Conditional Access.
* SQL authentication must not be used for the planned access model.
Azure Storage
* storage2 must support granular encryption for selected application data.
* The encryption change must not force all data in storage2 to use the same account-level encryption configuration.
* The solution must support future separation of encrypted data by workload.
Azure Functions
* Only Function Apps that process production workload data must be included in the implementation.
* Fa1 processes production AI transaction events and must be included.
* Fa2 is used only for diagnostics and test jobs and must not be included.
* Fa3 processes production security automation events and must be included.
Microsoft Defender for Cloud
* Applications hosted on AKS1 must be protected by the appropriate Defender for Cloud workload plan.
* The Defender for Cloud planned change must be delegated to the user with the least privilege required.
Azure Arc and Monitoring
* Server1 must be onboarded to Azure.
* Security telemetry from Server1 must be collected centrally.

* The solution must support security monitoring through Azure-native tooling.

NEW QUESTION # 109
A company stores confidential training data used by machine learning models. Administrators need to ensure that encryption keys remain under organizational control rather than being fully managed by Microsoft. Which option should be selected?

- A. Customer-managed keys (CMK)
- B. Anonymous encryption
- C. Shared Access Signatures
- D. Platform-managed keys only

Answer: A

Explanation:
Customer-managed keys allow organizations to control key lifecycle management, rotation, and revocation using Azure Key Vault or Managed HSM. This provides additional control over encryption compared to platform-managed keys. Shared Access Signatures govern access permissions and do not manage encryption ownership.

NEW QUESTION # 110
.....