Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

https://www.2passeasy.com/dumps/SC-500/

NEW QUESTION 1
You have an Azure subscription named Sub1 that contains a storage account named storage1
Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled.
The security team at your company requires that all malicious files be processed automatically by a serverless workflow for quarantine and notification.
You need to ensure that the malware scan results trigger an automated response. The solution must minimize operational effort.
What should you configure?

A. An Azure Event Grid subscription
B. Diagnostic settings to send logs to a Log Analytics workspace
C. Lifecycle management policies
D. An Azure Monitor alert rule

Answer: A

Explanation:
The security team wants a serverless workflow to run when scan results are produced. Defender for Storage malware scanning emits events that can be subscribed to through Azure Event Grid, and Event Grid can trigger Azure Functions, Logic Apps, or other serverless handlers. Diagnostic settings and Log Analytics are useful for investigation but are not the lowest-effort event trigger for each malicious upload. Lifecycle policies are storage-management controls, not security remediation workflows. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. 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 > Defender for Storage; Microsoft Learn > Event Grid events for malware scanning results.

NEW QUESTION 2
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 an Azure subscription that contains two virtual machines named VM1 and VM2. Each virtual machine has system-assigned managed identity enabled.
You have an Azure Storage account named storage. Public access from all networks is enabled for storage1.
You need to ensure that VM1 and VM2 can access storage1.
Solution: You create a private endpoint on storage1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
A private endpoint changes network routing so clients reach the storage account over a private IP address, but it does not grant data-plane authorization. The scenario already allows public network access, so network reachability is not the missing component. VM1 and VM2 still need Azure RBAC assignments for their managed identities or another valid authentication path. Therefore, a private endpoint alone does not meet the goal. For this domain, least privilege means granting only the required data operation or allowing only the required network flow. The correct response avoids shared keys, broad peering, general contributor roles, or log-only controls when the scenario demands prevention, routing, event triggering, or account-specific configuration. 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 > private endpoints and storage access; Microsoft Learn > private endpoints provide network access, not authorization.

NEW QUESTION 3
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 an analytics rule.
Does this meet the goal?

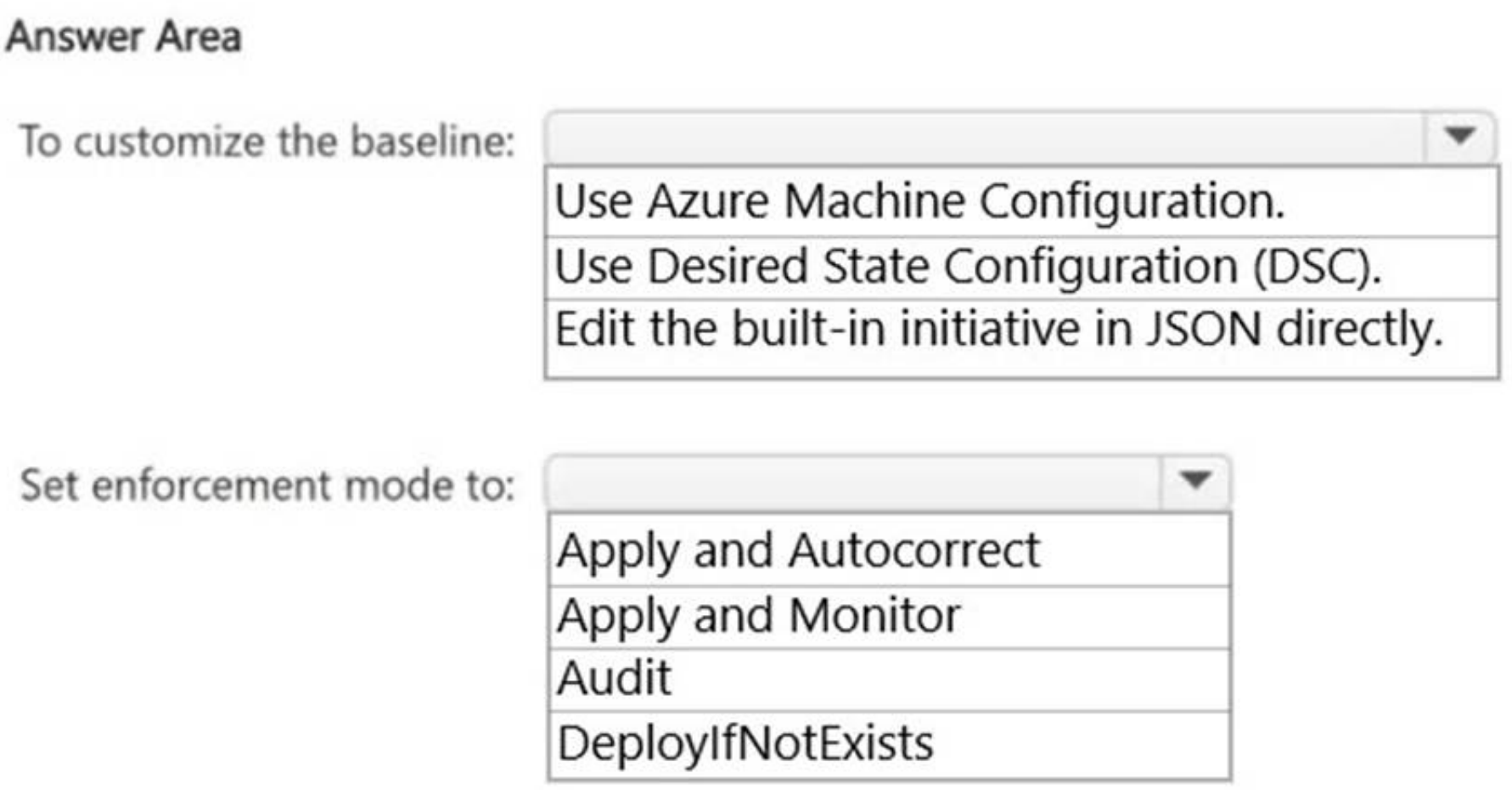
A. Yes
B. No

Answer: B

Explanation:
An analytics rule creates alerts and incidents from detection logic. It is not a global mechanism for assigning every new incident from all sources or adding triage flags after incident creation. While a specific analytics rule can set some incident details for incidents it generates, it does not meet the stated goal for all new incidents in the workspace. Sentinel automation rules or playbooks are the correct tools. In Microsoft Sentinel and Defender scenarios, collection, detection, investigation, and automation are separate functions. The selected answer maps to the function requested by the question rather than a neighboring capability. This is why analytics, hunting, workbooks, connectors, automation rules, and playbooks must not be treated as interchangeable. 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 > Sentinel analytics rules; Microsoft Learn > analytics rules create incidents, not global assignment handling.

NEW QUESTION 4
You have an Azure subscription that contains the following servers:
•200 virtual machines that run either Windows Server or Ubuntu Server
•50 Azure Arc enabled servers

You use Azure Policy to manage compliance across all the servers.
You need to enforce an organization-specific security baseline. The solution must meet the following requirements:
•Customize a built-in security baseline.
•Ensure that configuration changes to the servers are enforced automatically after the security baseline is deployed.
?Minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To customize the baseline: Use Azure Machine Configuration;
Set enforcement mode to: Apply and Autocorrect
Azure Machine Configuration is the correct mechanism for applying and customizing guest configuration baselines across Azure VMs and Azure Arc-enabled servers. It integrates with Azure Policy and can enforce configuration through assignment modes such as Apply and Autocorrect. This provides centralized compliance and automatic correction without building a separate configuration-management pipeline for Windows and Linux servers. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. 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 > Azure Machine Configuration; Microsoft Learn > assignment modes and remediation.

NEW QUESTION 5
You have Microsoft Security Copilot agents that authenticate by using Microsoft Entra service principals.
You receive a Microsoft Defender alert triggered by the anomalous OAuth authentication of an agent ' s Microsoft Entra service principal.
You need to assess the impact of the agent identity and identify which resources are affected if the identity is abused for lateral movement The solution must minimize administrative effort.
What should you do?

A. From Advanced hunting, create a query against the IdentityLogonEvents table to list all the sign-ins performed by the identity.
B. From Attack paths, select the identity and view the blast radius.
C. From AI Observability in Microsoft Purview Data Security Posture Management (DSPM), review the agent activity.
D. From Microsoft Purview Audit, query the audit logs for all the role assignments granted to the identity.
E. From Incidents, review incidents related to OAuth events reported by Microsoft Defender for Cloud Apps.

Answer: B

Explanation:
The security team needs impact and lateral-movement exposure for an abused service principal. Defender XDR attack paths show the identity blast radius by connecting permissions, exposed resources, and reachable assets. Advanced hunting and audit logs can provide raw evidence, but they require more manual analysis. AI Observability and incident review do not directly answer which resources are affected by identity abuse across the environment. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. 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 > analyze blast radius by using Defender XDR; Microsoft Learn > attack paths for identity risk.

NEW QUESTION 6
You have a Microsoft Entra tenant that has the following configurations:

•User consent for applications is disabled.
•Only administrators can grant permissions to applications.
You register an application named App1 that uses delegated Microsoft Graph permissions.
You need to configure App1 to meet the following requirements:
•Enable user sign-ins without interactive consent prompts.
•Enable App1 to access Microsoft Graph on behalf of the signed-in user.
What should you do?

A. Configure enterprise applications to require user assignment and assign users to App1.
B. Modify the app registration to use application permissions instead of delegated permissions.
C. Add the required delegated Microsoft Graph permissions to the app registration and rely on user consent during sign-in.
D. Grant admin consent to App1 for the required delegated permissions.

Answer: D

Explanation:
Delegated Microsoft Graph permissions allow an application to act on behalf of the signed-in user. Because user consent is disabled and only administrators may grant permissions, users cannot complete the consent prompt themselves. Granting admin consent for the required delegated permissions pre-authorizes the app and removes the interactive consent prompt while still preserving the delegated model. Switching to application permissions would change the operating model and grant app-only access. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. 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 > OAuth permission grants and consent; Microsoft Learn > admin consent for delegated permissions.

NEW QUESTION 7
You have a management group named MG1 that contains two subscriptions named Sub1 and Sub2
Sub1 contains a resource group named RG-Exception and a resource group named RG1 that hosts Microsoft Foundry resources.
You need to assign an Azure policy to force new Foundry deployments in MG1 to use private endpoints. The solution must NOT restrict deployments in RG-Exception.
How should you configure the policy?

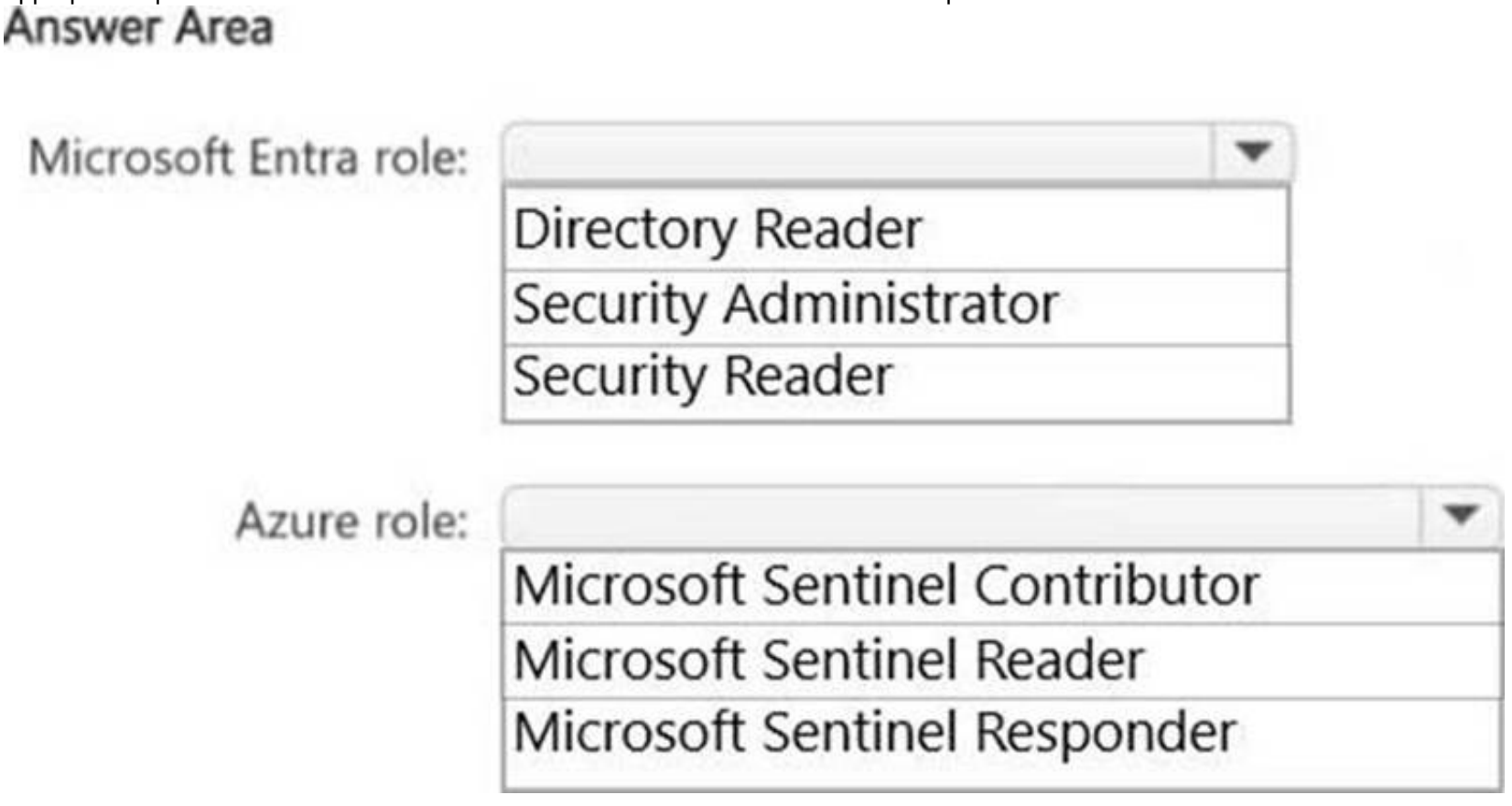
A. Assign the policy to MG1 and exclude RG-Exception.
B. Assign the policy to Sub1 and RG-Exception.
C. Assign the policy to MG1 and RG-Exception.
D. Assign the policy to Sub1 and exclude RG-Exception.

Answer: A

Explanation:
The policy must apply across the entire management group MG1 because both Sub1 and Sub2 are in scope for new Foundry deployments. The exception must be expressed as an exclusion for RG-Exception, not by assigning the policy directly to that resource group. Assigning only to Sub1 misses Sub2. Including RG-Exception in the assignment would restrict the resource group that the requirement explicitly excludes. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. 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 > Azure Policy; Microsoft Learn > policy assignment scopes and exclusions.

NEW QUESTION 8
HOTSPOT You have a Microsoft Sentinel workspace named Workspace1. You hire a security consultant. You provide the consultant with a guest account named User1 in your Microsoft Entra tenant. You need to enable User1 to assign incidents in Workspace1. Which roles should you assign to User1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Microsoft Entra role: Directory Reader
Azure role: Microsoft Sentinel Responder
Because User1 is a guest user, the Directory Reader role is required to assign Microsoft Sentinel incidents to users in the tenant. The Microsoft Sentinel Responder role grants the permissions needed to investigate and manage incidents, including updating incident ownership in Workspace1.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/roles
https://learn.microsoft.com/en-us/azure/sentinel/investigate-incidents

NEW QUESTION 9
HOTSPOT \You have an Azure subscription. \You need to create and deploy an Azure policy that meets the following requirements: - When a new virtual machine is deployed, automatically install a custom security extension. - Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension. What should you include in the policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Definition effect: DeployIfNotExists
For remediation, define: A managed identity that has the Contributor role
The DeployIfNotExists effect deploys the custom security extension when a virtual machine does not already have the required extension. Remediation tasks use the deployment template in this policy effect to correct existing non-compliant virtual machines. The policy assignment requires a managed identity with the permissions needed to deploy the extension; the Contributor role provides the required resource deployment permissions.
Reference:
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-deploy-if-not-exists
https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION 10
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 an Azure subscription that contains two virtual machines named VM1 and VM2. Each virtual machine has system-assigned managed identity enabled.
You have an Azure Storage account named storage1. Public access from all networks is enabled for storage1.
You need to ensure that VM1 and VM2 can access storage1.
Solution: You add each virtual machine to a security group, and then add the security group to a role on storage1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Adding virtual machines to a security group does not by itself grant Azure Storage access. The authorization principal used by Azure RBAC must be the managed identity or another supported security principal that the workload uses to request tokens. The solution also fails to state that the system-assigned managed identities are added to the group. Because the compute resources themselves are not the authenticating principals, this solution does not meet the goal. This domain is tested through precise scope control: tenant, subscription, resource, application, and data-plane authorization are not interchangeable. The correct

choice applies the smallest identity or governance control that enforces the stated requirement. Options that only add users, create registrations, or provide broad administrator access fail because they do not directly enforce the requested access behavior. 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 > Azure RBAC and identities; Microsoft Learn > role assignment requires an identity principal at the scope.

NEW QUESTION 10
You have a hybrid environment that contains the following servers:
•50 Azure virtual machines that run Windows Server 2019
•20 physical, on premises servers that run Windows Server 2019
All the servers use a third-party antivirus solution that must remain active during a phased security rollout
You need to onboard all the servers to Microsoft Defender for Endpoint by using a centralized deployment method. The solution must meet the following requirements:
•Endpoint detection and response (EDR) capabilities must be enabled.
•Antivirus conflicts must be prevented during onboarding.
What should you do on the servers?

A. Set the Microsoft Defender for Endpoint service to Disabled.
B. Disable Microsoft Defender Antivirus real-time protection by using Set-MpPreference.
C. Configure the ForceDefenderPassiveMode registry value.
D. Enable EDR in block mode.

Answer: C

NEW QUESTION 12
You have two management groups named MG1 and MG2 that contain multiple Azure subscriptions. The subscriptions are linked to a Microsoft Entra tenant.
You have a user named User1 and a global administrator named Admin 1
You are informed that User1 created an Azure subscription named Sub1 under the MG2 management group and is the only owner of the subscription.
You need to ensure that Admin1 can remove the Owner role from User1 for Sub1.
What should you do first?

A. Move Sub1 to MG1.
B. Assign Admin1 the User Access Administrator role for Sub1.
C. Instruct Admin1 to use Privileged Identity Management (PIM) to request the Security Administrator role.
D. Instruct Admin1 to enable Access management for Azure resources.

Answer: D

Explanation:
Enabling Access management for Azure resources allows a Microsoft Entra Global Administrator to
elevate access and receive the User Access Administrator role at the root scope. This inherited access applies to Sub1 and enables Admin1 to remove User1??s Owner role assignment from the subscription.
Reference:
https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin?tabs=azure-portal%2Centra-audit-logs
https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles

NEW QUESTION 14
For a site-to-site VPN connection to Azure, which protocol and configuration provide encrypted tunnels between on-premises and the Azure VPN gateway?

A. Plain HTTP over a public IP
B. FTP passive mode
C. IPsec/IKE policy on the VPN gateway
D. ICMP echo tunneling

Answer: C

Explanation:
Site-to-site VPNs to Azure use IPsec/IKE to establish encrypted tunnels between the on-premises VPN device and the Azure VPN gateway. Configuring a custom IPsec/IKE policy lets you enforce strong cipher suites and key exchange parameters.

NEW QUESTION 15
After an AI agent identity is suspected of compromise, which Defender XDR capability helps you analyze the potential blast radius of that Entra Agent ID?

A. Blast radius analysis for Entra Agent ID in Defender XDR
B. Storage lifecycle reports
C. Azure Cost alerts
D. Network Watcher packet capture

Answer: A

Explanation:
Defender XDR can analyze the blast radius of an Entra Agent ID, showing what resources and data the agent could reach if abused. Understanding this exposure helps responders scope containment and prioritize remediation for AI agents.

NEW QUESTION 19
You have a Microsoft Entra tenant that uses Privileged Identity Management (PIM). You need to modify the AI Administrator role settings to meet the following requirements: - Elevated access must be evaluated by another administrator before it is granted. - Privileged access must be removed automatically after a fixed period. Which two settings should you configure? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A.Require justification on activation

A. C.Expire eligible assignments after E.Expire active assignments after

Answer: BD

Explanation:
Requiring approval to activate ensures that a designated administrator must evaluate and approve an eligible user's elevation request before privileged access is granted. Setting an activation maximum duration makes each activated role assignment time-bound, automatically removing the elevated access when the configured activation period expires.
Reference:
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-activate-role

NEW QUESTION 23
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-500 Product From:

https://www.2passeasy.com/dumps/SC-500/

Money Back Guarantee

SC-500 Practice Exam Features:

* SC-500 Questions and Answers Updated Frequently

* SC-500 Practice Questions Verified by Expert Senior Certified Staff

* SC-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year