SC-100 Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sc-100.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 have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux.

You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:

Identify missing updates and insecure configurations. Use the Qualys engine.

What should you use?

A. Microsoft Defender for Servers

B. Microsoft Defender Threat Intelligence (Defender TI)

C. Microsoft Defender for Endpoint

D. Microsoft Defender External Attack Surface Management (Defender EASM)

Correct Answer: A

Explanation:

The vulnerability scanner included with Microsoft Defender for Cloud is powered by Qualys. Qualys\\' scanner is one of the leading tools for real-time identification of vulnerabilities. It\\'s only available with Microsoft Defender for Servers.

Note: Enable vulnerability scanning with the integrated Qualys scanner

A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Defender for Cloud regularly checks your connected machines to ensure they\\'re running vulnerability assessment tools.

When a machine is found that doesn\\'t have a vulnerability assessment solution deployed, Defender for Cloud generates the security recommendation: Machines should have a vulnerability assessment solution. Use this recommendation to

deploy the vulnerability assessment solution to your Azure virtual machines and your Azure Arc-enabled hybrid machines.

Defender for Cloud includes vulnerability scanning for your machines. You don\\'t need a Qualys license or even a Qualys account - everything\\'s handled seamlessly inside Defender for Cloud.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

QUESTION 2

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators groups on the Windows computers.

You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator

account on a computer is compromised.

What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

Correct Answer: A

Microsoft\\'s "Local Administrator Password Solution" (LAPS) provides management of local administrator account passwords for domain-joined computers. Passwords are randomized and stored in Active Directory (AD), protected by ACLs, so only eligible users can read it or request its reset.

Microsoft LAPS is short for Microsoft Local Administrator Password Solution. When installed and enabled on domain-joined computers it takes over the management of passwords of local accounts. Passwords are automatically changed to random characters that meet the domain\\'s password policy requirements at a frequency that you define through Group Policy.

The passwords are stored in a protected “confidential” attribute on the Computer object in AD. Unlike most other attributes which can be read by all domain users by default, the confidential attributes require extra privileges to be granted in order to read them, thus securing the managed passwords.

Incorrect: Not B: Integrate on-premises Active Directory domains with Azure Active Directory Validate security configuration and policy, Actively monitor Azure AD for signs of suspicious activity

Consider using Azure AD Premium P2 edition, which includes Azure AD Identity Protection. Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised. For example, it can detect potentially unusual activity such as irregular sign-in activities, sign-ins from unknown sources or from IP addresses with suspicious activity, or sign-ins from devices that may be infected. Identity Protection uses this data to generate reports and alerts that enable you to investigate these risk events and take appropriate action.

Not C: Azure AD PIM is a service in Azure AD that enables you to manage, control, and monitor access to resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Not D: Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides very strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket.

Reference: https://craighays.com/microsoft-laps/ https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

QUESTION 3

HOTSPOT

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to evaluate the existing environment to increase the overall security posture for the following components:

1.

Windows 11 devices managed by Microsoft Intune

2.

Azure Storage accounts

3.

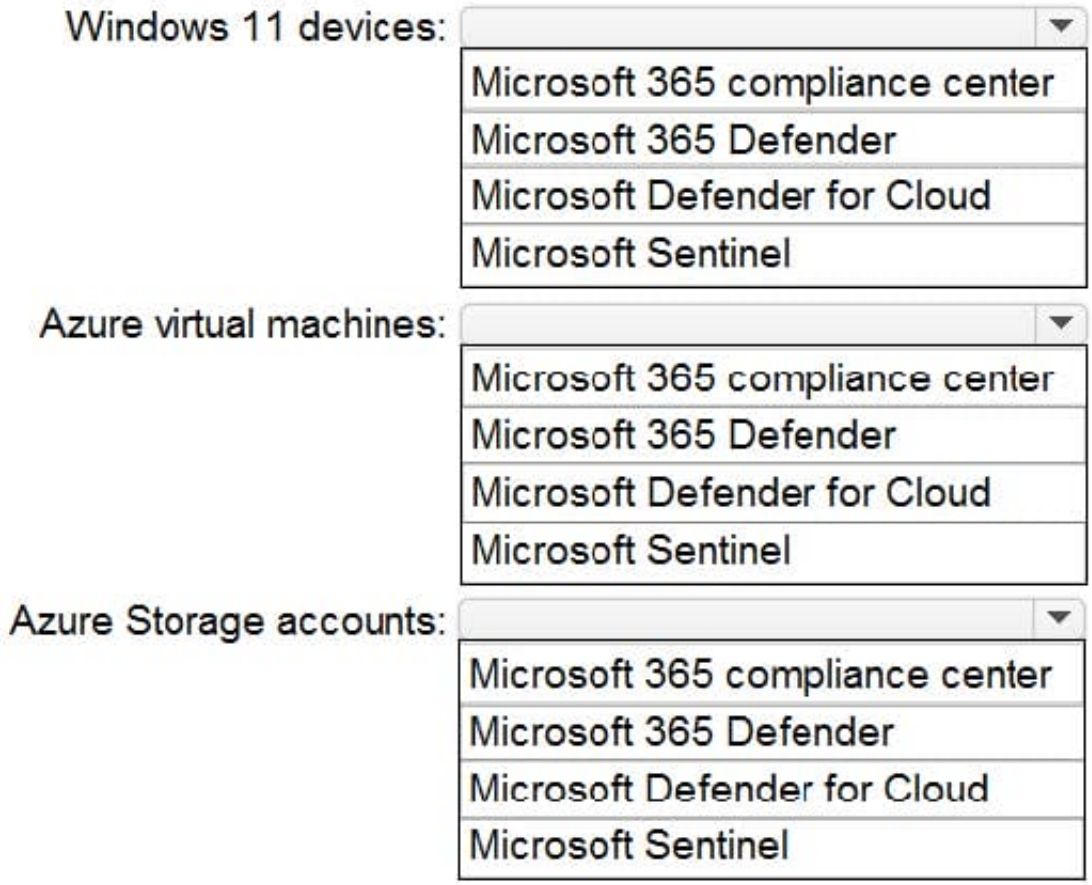
Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

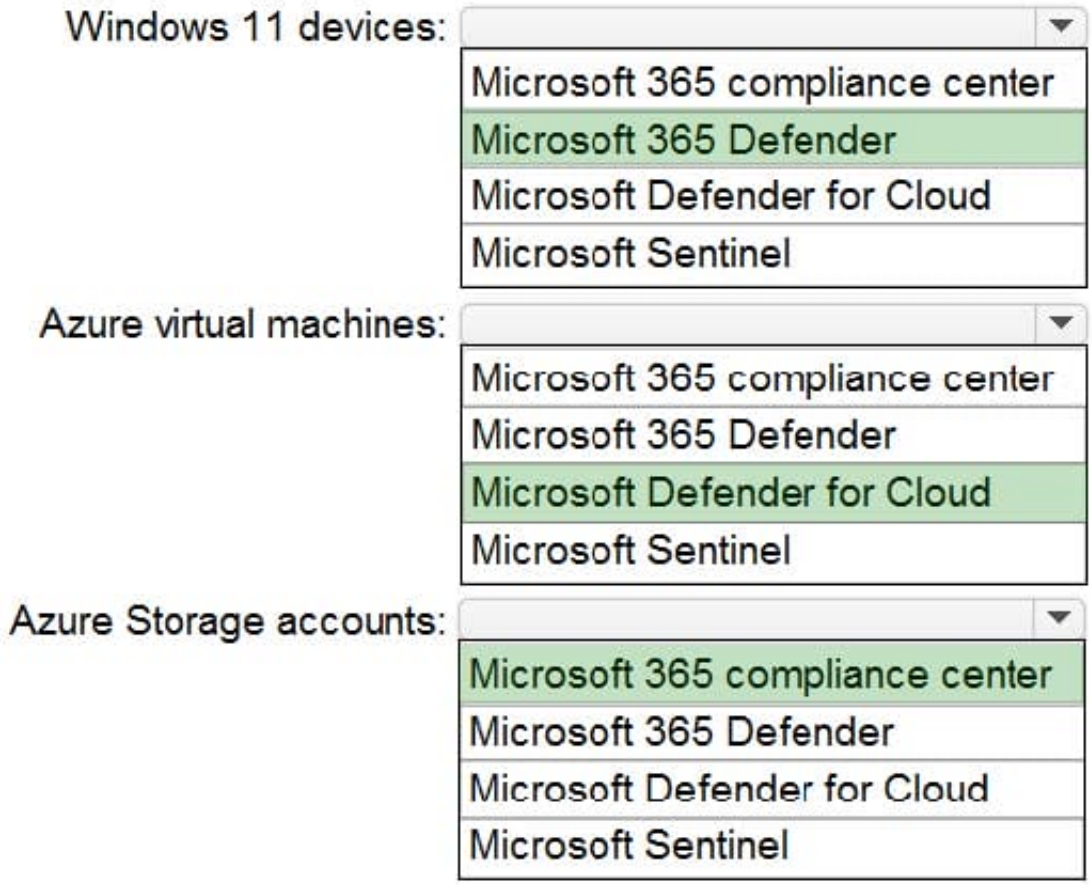
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Microsoft 365 Defender

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Microsoft Defender for Endpoint works with devices that run:

Android

iOS/iPadOS

Windows 10

Windows 11

Box 2: Microsoft Defender for Cloud

Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed

Instance and Azure Virtual Machines.

Box 3: Microsoft 365 Compliance Center

Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.

Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.

Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.

Reference: https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint

https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

QUESTION 4

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

What should you include in the recommendation?

A. Apply read-only locks on the storage accounts.

B. Set the AllowSharcdKeyAccess property to false.

C. Set the AllowBlobPublicAcccss property to false.

D. Configure automated key rotation.

Correct Answer: A

A read-only lock on a storage account prevents users from listing the account keys. A POST request handles the Azure Storage List Keys operation to protect access to the account keys. The account keys provide complete access to data in

the storage account.

Incorrect:

Not A:

If any clients are currently accessing data in your storage account with Shared Key, then Microsoft recommends that you migrate those clients to Azure AD before disallowing Shared Key access to the storage account.

However, in this scenario we cannot migrate to Azure AD due to the legacy applications.

Note: Shared Key

A shared key is a very long string. You can simply access Azure storage by using this long string. It\\'s almost like a password. Actually, it\\'s worse: this is a master password. It gives you all sorts of rights on the Azure storage account. You can

imagine why this isn\\'t my favorite mechanism of accessing Azure storage. What happens when this key is compromised? You don\\'t get an alert. Perhaps you can set up monitoring to see misuse of your Azure storage account. But it\\'s still less

than an ideal situation. Alerts will tell you of damage after it has already occurred.

Not C: Data breaches caused by cloud misconfiguration have been seen for the past few years. One of the most common misconfigurations is granting public access to cloud storage service. Such a data is often unprotected, making them to

be accessed without any authentication method. Microsoft recently introduced a new protection feature to help avoid public access on storage account. The feature introduces a new property named allowBlobPublicAccess.

Not D: Key rotation would improve security.

Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency.

You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.

This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault.

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

https://docs.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent

https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

QUESTION 5

You are designing the security standards for containerized applications onboarded to Azure.

You are evaluating the use of Microsoft Defender for Containers.

In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Instances

B. Windows containers deployed to Azure Kubernetes Service (AKS)

C. Windows containers deployed to Azure Container Registry

D. Linux containers deployed to Azure Container Registry

E. Linux containers deployed to Azure Kubernetes Service (AKS)

Correct Answer: DE

https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=azure-aks#registries-and-images Windows is on preview.

OS Packages Supported

- Alpine Linux 3.12-3.15
- Red Hat Enterprise Linux 6, 7, 8
- CentOS 6, 7
- Oracle Linux 6,6,7,8
- Amazon Linux 1,2 • openSUSE Leap 42, 15
- SUSE Enterprise Linux 11,12, 15
- Debian GNU/Linux wheezy, jessie, stretch, buster, bullseye
- Ubuntu 10.10-22.04
- FreeBSD 11.1-13.1
- Fedora 32, 33, 34, 35