SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

https://www.geekcert.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 need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.

Which two services should you leverage in the strategy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. access reviews in Azure AD

C. Microsoft Defender for Cloud

D. Microsoft Defender for Cloud Apps

E. Microsoft Defender for Endpoint

Correct Answer: BD

Scenario: Litware identifies the following application security requirements:

Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

B: Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User\\'s access can be reviewed on a regular basis to make sure only the right people have continued access.

D: The Defender for Cloud Apps framework Discover and control the use of Shadow IT: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.

Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real time across all your cloud apps.

Etc.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview
https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

QUESTION 2

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups. Recommendations:

-Internet-facing virtual machines should be protected with network security groups

-

Management ports of virtual machines should be protected with just-in-time network access control

-

Management ports should be closed on your virtual machines Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 3

HOTSPOT

You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

1.

A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers

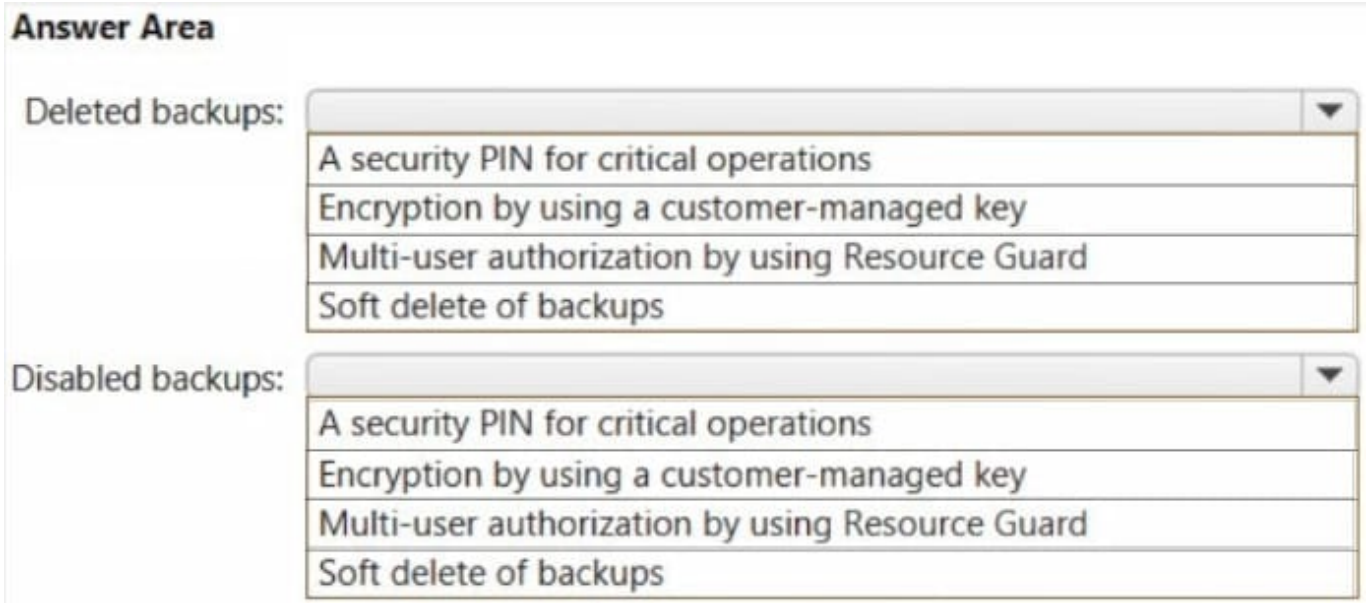
2.

A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

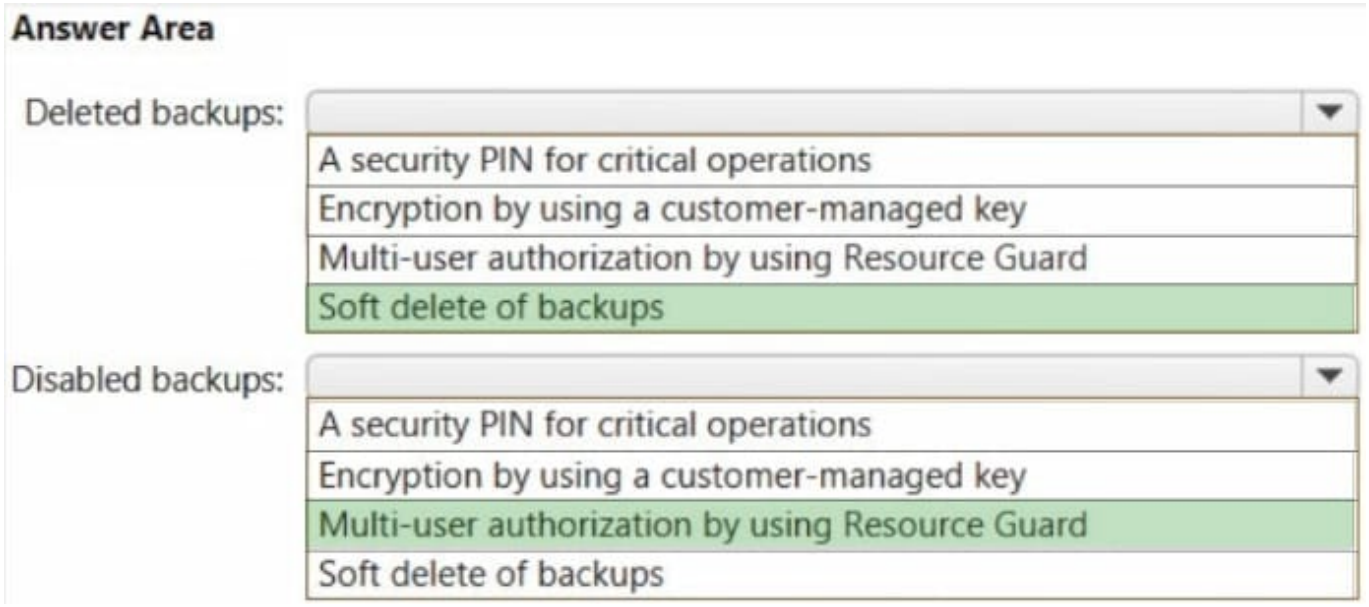
What should you use for each risk? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Soft delete of backups

How to block intentional or unintentional deletion of backup data?

Enable Soft delete is enabled to protect backups from accidental or malicious deletes.

Soft delete is a useful feature that helps you deal with data loss. Soft delete retains backup data for 14 days, allowing the recovery of that backup item before it\\'s permanently lost.

Box 2: Multi-user authorization by using Resource Guard

Ensure Multi-user authorization (MUA) is enabled for an additional layer of protection.

MUA for Azure Backup uses a new resource called Resource Guard to ensure critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, are performed only with applicable

authorization.

Reference: https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

QUESTION 4

Reference: https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.

Note:

Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.

Recommendations:

-Internet-facing virtual machines should be protected with network security groups

-

Management ports of virtual machines should be protected with just-in-time network access control

-

Management ports should be closed on your virtual machines Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 5

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator

authorizes the application.

Which security control should you recommend?

A. app registrations in Azure Active Directory (Azure AD)

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. Azure Security Benchmark compliance controls in Defender for Cloud

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: B

Microsoft Defender for Cloud Apps OAuth app policies.

OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and Salesforce. You\\'re also able to mark these permissions as approved or banned.

Marking them as banned will revoke permissions for each app for each user who authorized it.

Incorrect:

Not D: Windows Defender Application cannot be used for virtual machines.

Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/app-permission-policy