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.pass2lead.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 a Microsoft 365 E5 subscription.

You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.

You need to recommend a solution to prevent Personally Identifiable Information (Pll) from being shared.

Which two components should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies

B. retention label policies

C. eDiscovery cases

D. sensitivity label policies

Correct Answer: AD

A: Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your

organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically

protect sensitive information across Office 365.

D: Sensitivity labels

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization\\'s data without hindering the productivity of users and their ability to collaborate.

Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud

Apps.

Incorrect:

Not B: Retention labels help you retain what you need and delete what you don\\'t at the item level (document or email). They are also used to declare an item as a record as part of a records management solution for your Microsoft 365 data.

Not C: eDiscovery cases in eDiscovery (Standard) and eDiscovery (Premium) let you associate specific searches and exports with a specific investigation. You can also assign members to a case to control who can access the case and view

the contents of the case. Place content locations on legal hold.

Reference: https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/ https://docs.mic

rosoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

QUESTION 2

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 discovery anomaly detection policies in Microsoft Defender for Cloud Apps

B. Azure AD Conditional Access App Control policies

C. adaptive application controls in Defender for Cloud

D. app protection policies in Microsoft Endpoint Manager

Correct Answer: C

Explanation:

Use adaptive application controls to reduce your machines\\' attack surfaces

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

When you\\'ve enabled and configured adaptive application controls, you\\'ll get security alerts if any application runs other than the ones you\\'ve defined as safe.

Incorrect:

Not A: A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are

considered for each cloud application. Each increase is compared to the normal usage pattern of the application as learned from past usage. The most extreme increases trigger security alerts.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

QUESTION 3

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.

Correct Answer: ACE

QUESTION 4

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

A. Azure Firewall

B. Azure Web Application Firewall (WAF)

C. Microsoft Defender for Cloud alerts

D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)

E. Microsoft Sentinel

Correct Answer: AB

This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secure score. Sentinel and PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 5

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity.

You are informed about incidents that relate to compromised identities.

You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered.

Which Defender for Identity feature should you include in the recommendation?

A. sensitivity labels

B. custom user tags

C. standalone sensors

D. honeytoken entity tags

Correct Answer: D

Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.

Incorrect:

Not B: custom user tags

After you apply system tags or custom tags to users, you can use those tags as filters in alerts, reports, and investigation.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-identity/entity-tags