SC-100^{Q&As}

Microsoft Cybersecurity Architect

QUESTION 1

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

Correct Answer: B

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

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: A

The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in NIST SP 800-53 Rev. 5.

The following mappings are to the NIST SP 800-53 Rev. 5 controls. Use the navigation on the right to jump directly to a specific compliance domain. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open Policy in the Azure portal and select the Definitions page. Then, find and select the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative definition. Reference: https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

QUESTION 4

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

A. row-level security (RLS)

B. Transparent Data Encryption (TDE)

C. Always Encrypted

D. data classification

E. dynamic data masking

Correct Answer: C

Anyone with admin privileges can see masked data. https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-enclaves

QUESTION 5

You have an Azure subscription.

You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar.

Developers use Azure DevOps to deploy web apps to App Service Environments. When a new app is deployed, a CNAME record for the app is registered in contoso.com.

You need to recommend a solution to secure the DNS record for each web app. The solution must meet the following requirements:

- Ensure that when an app is deleted, the CNAME record for the app is removed also.

- Minimize administrative effort.

What should you include in the recommendation?

A.

Microsoft Defender for Cloud Apps

B.

Microsoft Defender for DevOps

C.

Microsoft Defender for App Service

D.

Microsoft Defender for DNS

Correct Answer: C