

Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect



NEW QUESTION 1

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 the VMAccess extension on all virtual machines.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s> Adaptive Network Hardening:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

NEW QUESTION 2

- (Exam Topic 3)

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

- A. the Azure landing zone accelerator
- B. the Azure Well-Architected Framework
- C. Azure Security Benchmark v3
- D. Azure Advisor

Answer: A

NEW QUESTION 3

- (Exam Topic 3)

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions that allow traffic from the Front Door service tags. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure>

NEW QUESTION 4

- (Exam Topic 3)

You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:

- Encrypt cardholder data by using encryption keys managed by the company.
- Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
- B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
- C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
- D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

Answer: AC

Explanation:

<https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service-encryption/>

NEW QUESTION 5

- (Exam Topic 3)

You have a Microsoft 365 subscription.

You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

Which two services should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Microsoft Defender for Cloud Apps
- B. Azure AD Application Proxy
- C. Azure Data Catalog

- D. Azure AD Conditional Access
- E. Microsoft Purview Information Protection

Answer: AD

NEW QUESTION 6

- (Exam Topic 3)

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription. All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

- Ensure that the security operations team can access the security logs and the operation logs.
- Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.

Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Active Directory (Azure AD) Conditional Access policies
- B. a custom collector that uses the Log Analytics agent
- C. resource-based role-based access control (RBAC)
- D. the Azure Monitor agent

Answer: CD

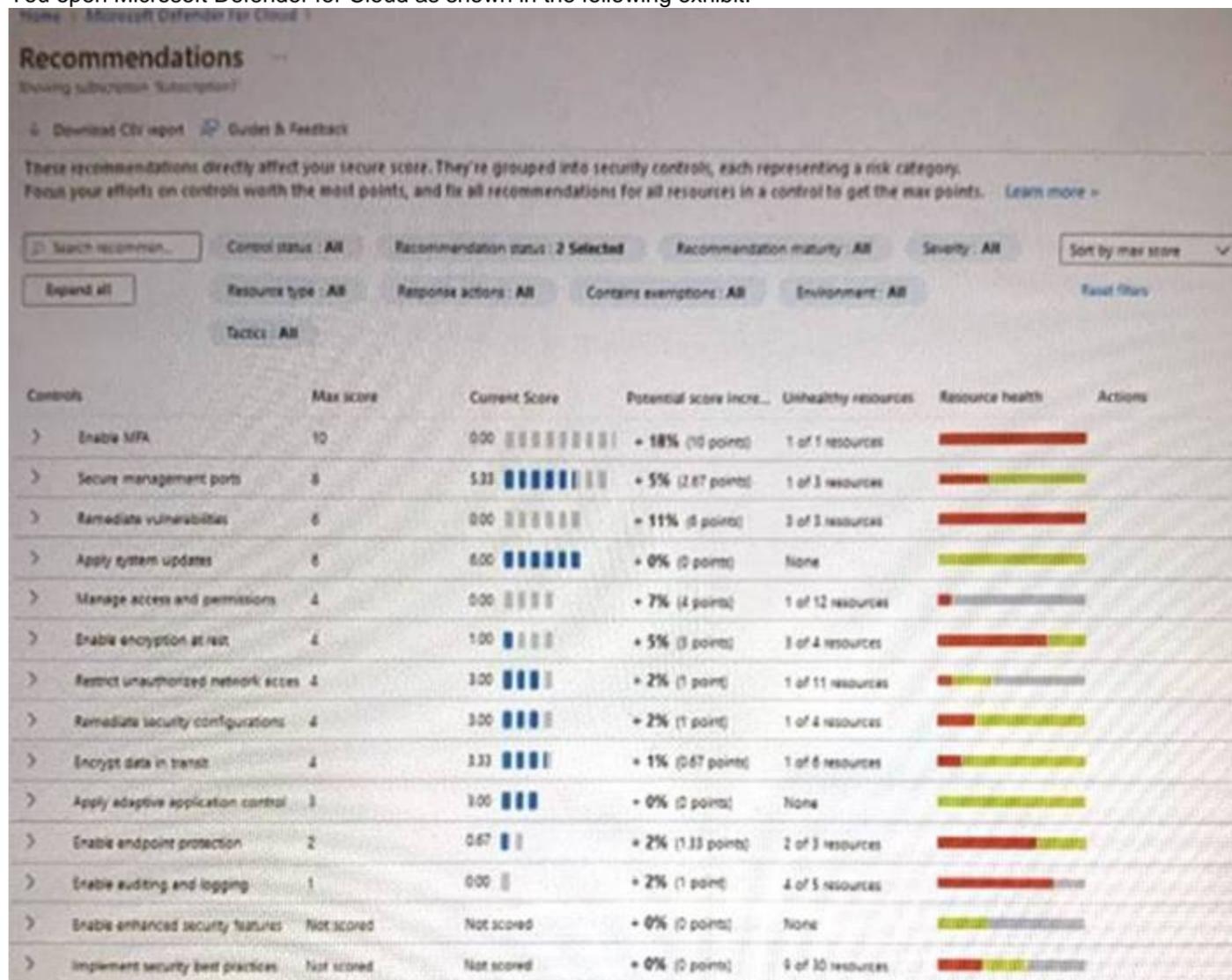
Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent>

NEW QUESTION 7

- (Exam Topic 3)

You open Microsoft Defender for Cloud as shown in the following exhibit.



Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Selection 1: NSG Selection

Selection 2: Microsoft Defender for servers

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

NEW QUESTION 8

- (Exam Topic 3)

You have Microsoft Defender for Cloud assigned to Azure management groups. You have a Microsoft Sentinel deployment.

During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. workload protections in Defender for Cloud
- B. threat intelligence reports in Defender for Cloud
- C. Microsoft Sentinel notebooks
- D. Microsoft Sentinel threat intelligence workbooks

Answer: BD

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports> <https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

NEW QUESTION 9

- (Exam Topic 3)

Azure subscription that uses Azure Storage.

The company plans to share specific blobs with vendors. You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be time-limited. What should you include in the recommendation?

- A. Create shared access signatures (SAS).
- B. Share the connection string of the access key.
- C. Configure private link connections.
- D. Configure encryption by using customer-managed keys (CMKs)

Answer: D

NEW QUESTION 10

- (Exam Topic 3)

You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.

You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

- A. Microsoft Information Protection
- B. Microsoft Defender for Endpoint
- C. Microsoft Sentinel
- D. Microsoft Endpoint Manager

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboa>

NEW QUESTION 10

- (Exam Topic 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.

Answer: ACE

NEW QUESTION 12

- (Exam Topic 3)

You are designing the security architecture for a cloud-only environment.

You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

- Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
- Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct

selection is worth one point.

Answer Area

DLP:
 Azure Data Catalog
 Azure Data Explorer
 Microsoft Purview

UEBA:
 Azure AD Identity Protection
 Microsoft Defender for Identity
 Microsoft Entra Verified ID

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

DLP:
 Azure Data Catalog
 Azure Data Explorer
 Microsoft Purview

UEBA:
 Azure AD Identity Protection
 Microsoft Defender for Identity
 Microsoft Entra Verified ID

NEW QUESTION 15

- (Exam Topic 3)

Your company has on-premises Microsoft SQL Server databases. The company plans to move the databases to Azure. You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs. What should you include in the recommendation?

- A. Azure SQL Managed Instance
- B. Azure Synapse Analytics dedicated SQL pools
- C. Azure SQL Database
- D. SQL Server on Azure Virtual Machines

Answer: C

NEW QUESTION 18

- (Exam Topic 3)

You are designing a ransomware response plan that follows Microsoft Security Best Practices. You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out. What should you include in the recommendations?

- A. Privileged Access Workstations (PAWs)
- B. emergency access accounts
- C. device compliance policies
- D. Customer Lockbox for Microsoft Azure

Answer: B

NEW QUESTION 21

- (Exam Topic 3)

You are planning the security levels for a security access strategy. You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security level should you configure for each job role? 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:

Answer Area



NEW QUESTION 23

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised administrator account cannot be used to delete the backups. What should you do?

- A. From a Recovery Services vault generate a security PIN for critical operations.
- B. From Azure Backup, configure multi-user authorization by using Resource Guard.
- C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.
- D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

Answer: B

NEW QUESTION 28

- (Exam Topic 3)

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 (PII) 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. sensitivity label policies
- C. retention label policies
- D. eDiscovery cases

Answer: AB

Explanation:

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.

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 alongside capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.
<https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/> <https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?vie>

NEW QUESTION 30

- (Exam Topic 3)

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service. You are migrating the on-premises infrastructure to a cloud-only infrastructure.

You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.

Which identity service should you include in the recommendation?

- A. Azure Active Directory Domain Services (Azure AD DS)
- B. Azure Active Directory (Azure AD) B2C
- C. Azure Active Directory (Azure AD)
- D. Active Directory Domain Services (AD DS)

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview>

NEW QUESTION 32

- (Exam Topic 3)

You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.

You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:

- Automatically identify threats found in AWS CloudTrail events.
- Enforce security settings on AWS virtual machines by using Azure policies.

What should you include in the solution for each requirement? 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:

Answer Area



NEW QUESTION 33

- (Exam Topic 3)

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online, SharePoint Online, and Teams in near-real-time (NRT) in response to the following Azure AD events:

- A user account is disabled or deleted
- The password of a user is changed or reset.
- All the refresh tokens for a user are revoked
- Multi-factor authentication (MFA) is enabled for a user

Which two features should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. continuous access evaluation
- B. a sign-in risk policy
- C. Azure AD Privileged Identity Management (PIM)
- D. Conditional Access
- E. Azure AD Application Proxy

Answer: AD

NEW QUESTION 35

- (Exam Topic 3)

You have Windows 11 devices and Microsoft 365 E5 licenses.

You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

- A. Microsoft Endpoint Manager
- B. Compliance Manager
- C. Microsoft Defender for Cloud Apps
- D. Microsoft Defender for Endpoint

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-w>

NEW QUESTION 39

- (Exam Topic 3)

You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:

- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts. You need to recommend an access security architecture for App1.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To enable Azure AD authentication for App1, use:

<input type="checkbox"/>	Azure AD application
<input type="checkbox"/>	Azure AD Application Proxy
<input type="checkbox"/>	Azure Application Gateway
<input type="checkbox"/>	A managed identity in Azure AD
<input type="checkbox"/>	Microsoft Defender for App

To implement access requests for App1, use:

<input type="checkbox"/>	An access package in Identity Governance
<input type="checkbox"/>	An access policy in Microsoft Defender for Cloud Apps
<input type="checkbox"/>	An access review in Identity Governance
<input type="checkbox"/>	Azure AD Conditional Access App Control
<input type="checkbox"/>	An OAuth app policy in Microsoft Defender for Cloud Apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1 is the Azure AD Application

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

Box 2 is Access Package in Identity Governance

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cr>

NEW QUESTION 43

- (Exam Topic 3)

Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices. You plan to use security baselines from the Microsoft Security Compliance Toolkit.

What should you recommend using to compare the baselines to the current device configurations?

- A. Microsoft Intune
- B. Policy Analyzer
- C. Local Group Policy Object (LGPO)
- D. Windows Autopilot

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework>

NEW QUESTION 45

- (Exam Topic 3)

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

- Microsoft SharePoint Online
- Microsoft Exchange Online
- Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Scopes

- Files and emails
- Groups and sites
- Schematized data assets

Answer Area

- SharePoint Online: Scope
- Microsoft Teams: Scope
- Exchange Online: Scope

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails –

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide> Go to label scopes

NEW QUESTION 47

- (Exam Topic 2)

You need to recommend a multi-tenant and hybrid security solution that meets the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

NEW QUESTION 49

- (Exam Topic 2)

You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.

What should you recommend? 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:

Segment Microsoft Sentinel workspaces by: Region and Azure AD tenant Lighthouse subscription

NEW QUESTION 50

- (Exam Topic 1)

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation? (Choose Two)

- A. Onboard the virtual machines to Microsoft Defender for Endpoint.
- B. Onboard the virtual machines to Azure Arc.
- C. Create a device compliance policy in Microsoft Endpoint Manager.
- D. Enable the Qualys scanner in Defender for Cloud.

Answer: AC

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365->

NEW QUESTION 55

- (Exam Topic 1)

You need to recommend a solution to meet the compliance requirements.

What should you recommend? 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:

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with> <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure>

while it is in policy assignment

- <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure>

NEW QUESTION 59

- (Exam Topic 3)

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Azure AD Conditional Access integration with user flows and custom policies
- B. Azure AD workbooks to monitor risk detections
- C. custom resource owner password credentials (ROPC) flows in Azure AD B2C
- D. access packages in Identity Governance
- E. smart account lockout in Azure AD B2C

Answer: AC

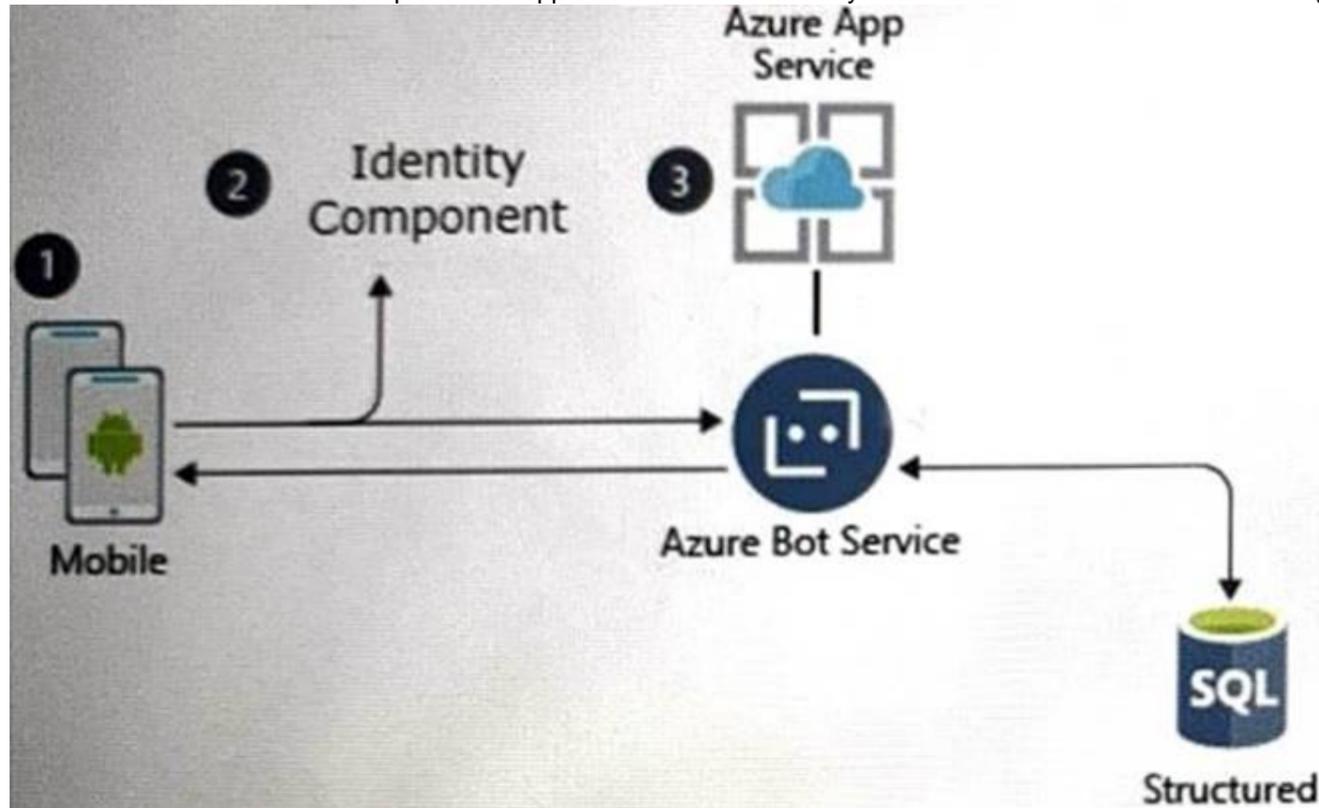
Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management>
<https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow>

NEW QUESTION 62

- (Exam Topic 3)

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

- Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
- Be managed separately from the identity store of the customer.
- Support fully customizable branding for each app.

Which service should you recommend to complete the design?

- A. Azure Active Directory (Azure AD) B2C
- B. Azure Active Directory (Azure AD) B2B
- C. Azure AD Connect
- D. Azure Active Directory Domain Services (Azure AD DS)

Answer: A

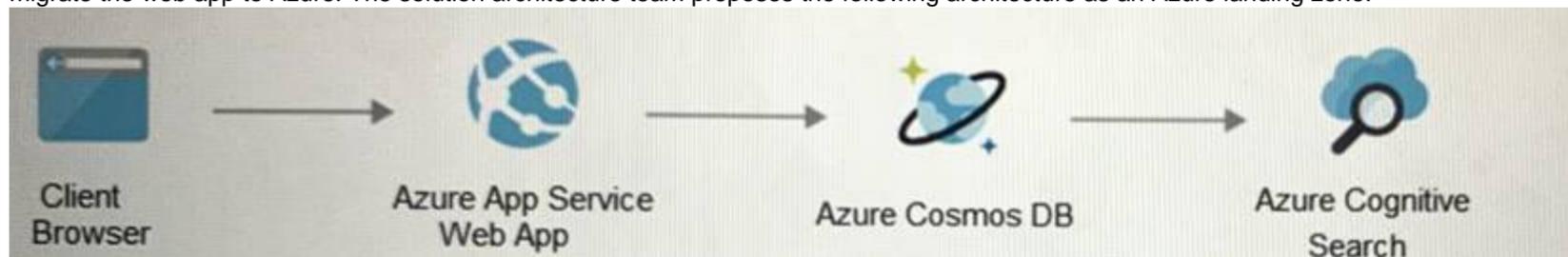
Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow> <https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow>

NEW QUESTION 64

- (Exam Topic 3)

Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data

exchanges are over the private IP space and the traffic never leaves the Microsoft network.

NEW QUESTION 69

- (Exam Topic 3)

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1. What should you include in the design?

- A. Azure AD Application Proxy
- B. connected apps in Microsoft Defender for Cloud Apps
- C. Microsoft Entra Identity Governance
- D. access policies in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 71

- (Exam Topic 3)

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (O/CD) workflows for the deployment of applications to Azure. You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure. What should you recommend?

- A. unit testing
- B. penetration testing
- C. dependency testing
- D. threat modeling

Answer: C

NEW QUESTION 75

- (Exam Topic 3)

Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

- Minimizes manual intervention by security operation analysts
- Supports Waging alerts within Microsoft Teams channels What should you include in the strategy?

- A. data connectors
- B. playbooks
- C. workbooks
- D. KQL

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC>

NEW QUESTION 80

- (Exam Topic 3)

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices. You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

- A. controlled folder access
- B. application isolation
- C. memory scanning
- D. machine isolation
- E. user isolation

Answer: D

NEW QUESTION 81

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Service:

- Azure AD Identity Protection
- Microsoft Defender for DNS
- Microsoft Defender for Office 365**
- Microsoft Purview

Policy type:

- Anti-phishing**
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Service:

- Azure AD Identity Protection
- Microsoft Defender for DNS
- Microsoft Defender for Office 365**
- Microsoft Purview

Policy type:

- Anti-phishing**
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

NEW QUESTION 86

- (Exam Topic 3)

Your company plans to provision blob storage by using an Azure Storage account. The blob storage will be accessible from 20 application servers on the internet. You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

- A. service tags in network security groups (NSGs)
- B. managed rule sets in Azure Web Application Firewall (WAF) policies
- C. inbound rules in network security groups (NSGs)
- D. firewall rules for the storage account
- E. inbound rules in Azure Firewall

Answer: D

NEW QUESTION 88

- (Exam Topic 3)

You design cloud-based software as a service (SaaS) solutions.

You need to recommend ransomware attacks. The solution must follow Microsoft Security Best Practices. What should you recommend doing first?

- A. Implement data protection.
- B. Develop a privileged access strategy.
- C. Prepare a recovery plan.
- D. Develop a privileged identity strategy.

Answer: C

NEW QUESTION 91

- (Exam Topic 3)

Your company wants to optimize using Azure to protect its resources from ransomware.

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Azure Backup: Encryption by using platform-managed keys
 Access policies
 Access tiers
Encryption by using platform-managed keys
 Immutable storage
 A security PIN

Azure Storage: Immutable storage
 Access policies
 Access tiers
 Encryption by using platform-managed keys
Immutable storage
 A security PIN

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure Backup: Encryption by using platform-managed keys
 Access policies
 Access tiers
Encryption by using platform-managed keys
 Immutable storage
 A security PIN

Azure Storage: Immutable storage
 Access policies
 Access tiers
 Encryption by using platform-managed keys
Immutable storage
 A security PIN

NEW QUESTION 94

- (Exam Topic 3)

You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect f personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG) You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:

- Ensure that each time the support staff connects to a jump server; they must request access to the server.
- Ensure that only authorized support staff can initiate SSH connections to the jump servers.
- Maximize protection against brute-force attacks from internal networks and the internet.
- Ensure that users can only connect to the jump servers from the internet.
- Minimize administrative effort

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Manage NSG rules by using: Just-in-time (JIT) VM access
 Azure Automation
 Azure Bastion
Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established
Any public IP addresses provided before the connection is established
 AzureBastionSubnet
 GatewaySubnet

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Manage NSG rules by using: Just-in-time (JIT) VM access
 Azure Automation
 Azure Bastion
Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established
Any public IP addresses provided before the connection is established
 AzureBastionSubnet
 GatewaySubnet

NEW QUESTION 95

- (Exam Topic 3)

You have legacy operational technology (OT) devices and IoT devices.

You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures

(MCRA). The solution must minimize the risk of disrupting business operations.

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

NOTE: Each correct selection is worth one point

- A. passive traffic monitoring
- B. active scanning
- C. threat monitoring
- D. software patching

Answer: CD

NEW QUESTION 98

- (Exam Topic 3)

You have an on-premises network and a Microsoft 365 subscription. You are designing a Zero Trust security strategy.

Which two security controls should you include as part of the Zero Trust solution? Each correct answer part of the solution.

NOTE: Each correct answer is worth one point.

- A. Block sign-attempts from unknown location.
- B. Always allow connections from the on-premises network.
- C. Disable passwordless sign-in for sensitive account.
- D. Block sign-in attempts from noncompliant devices.

Answer: AD

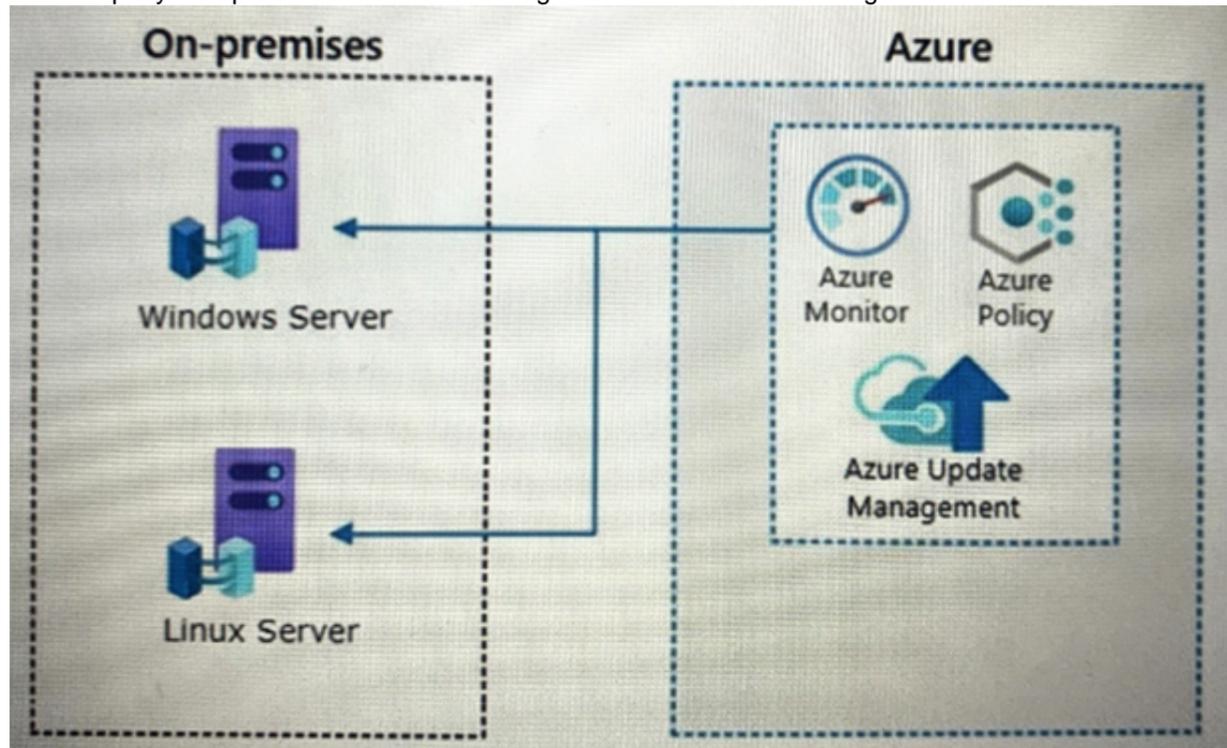
NEW QUESTION 102

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:

- > Govern virtual machines and servers across multiple environments.
- > Enforce standards for all the resources across all the environment across the Azure policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

- A. Azure VPN Gateway
- B. guest configuration in Azure Policy
- C. on-premises data gateway
- D. Azure Bastion
- E. Azure Arc

Answer: BE

Explanation:

<https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview>

NEW QUESTION 107

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:

- Identify unused personal data and empower users to make smart data handling decisions.
- Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
- Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

- A. Microsoft Viva Insights

- B. Advanced eDiscovery
- C. Privacy Risk Management in Microsoft Priva
- D. communication compliance in insider risk management

Answer: C

Explanation:

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you: Detect overexposed personal data so that users can secure it. Spot and limit transfers of personal data across departments or regional borders. Help users identify and reduce the amount of unused personal data that you store.
<https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management>

NEW QUESTION 109

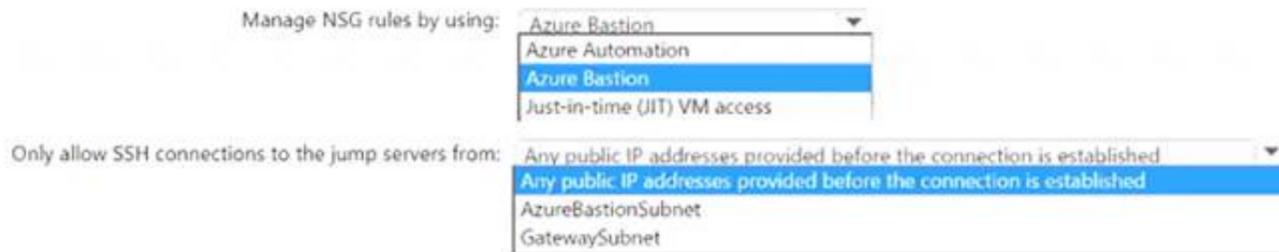
- (Exam Topic 3)

You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG). You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:

- Ensure that each time the support staff connects to a jump server; they must request access to the server.
- Ensure that only authorized support staff can initiate SSH connections to the jump servers.
- Maximize protection against brute-force attacks from internal networks and the internet.
- Ensure that users can only connect to the jump servers from the internet.
- Minimize administrative effort.

What should you include in the solution? 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:

Answer Area



NEW QUESTION 110

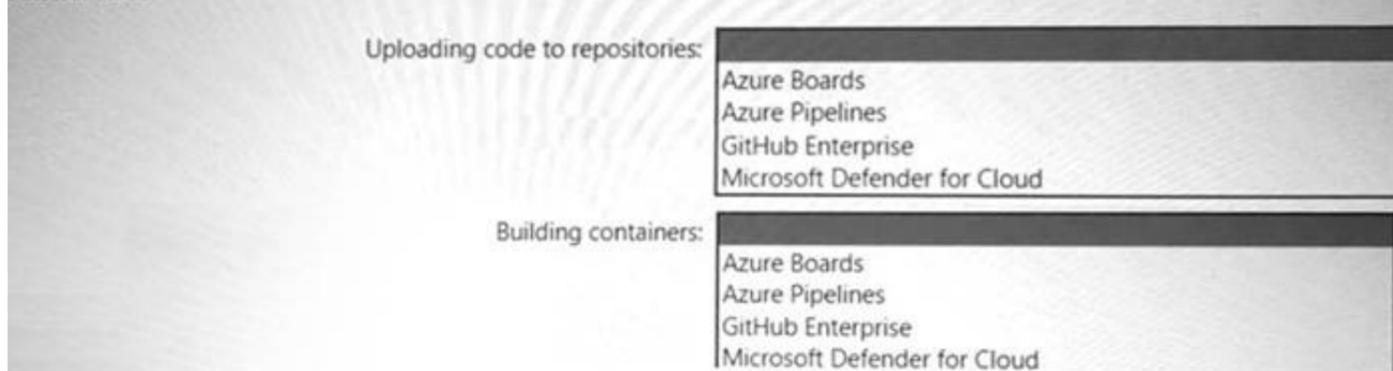
- (Exam Topic 3)

Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:

Uploading the code to repositories Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec> <https://microsoft.github.io/code-with-engineering->

playbook/automated-testing/tech-specific-samples/azdo-conta

NEW QUESTION 115

- (Exam Topic 3)

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)

Answer: A

NEW QUESTION 118

- (Exam Topic 3)

Your company is moving a big data solution to Azure. The company plans to use the following storage workloads:

- Azure Storage blob containers
- Azure Data Lake Storage Gen2
- Azure Storage file shares
- Azure Disk Storage

Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Disk Storage
- B. Azure Storage blob containers
- C. Azure Storage file shares
- D. Azure Data Lake Storage Gen2

Answer: BD

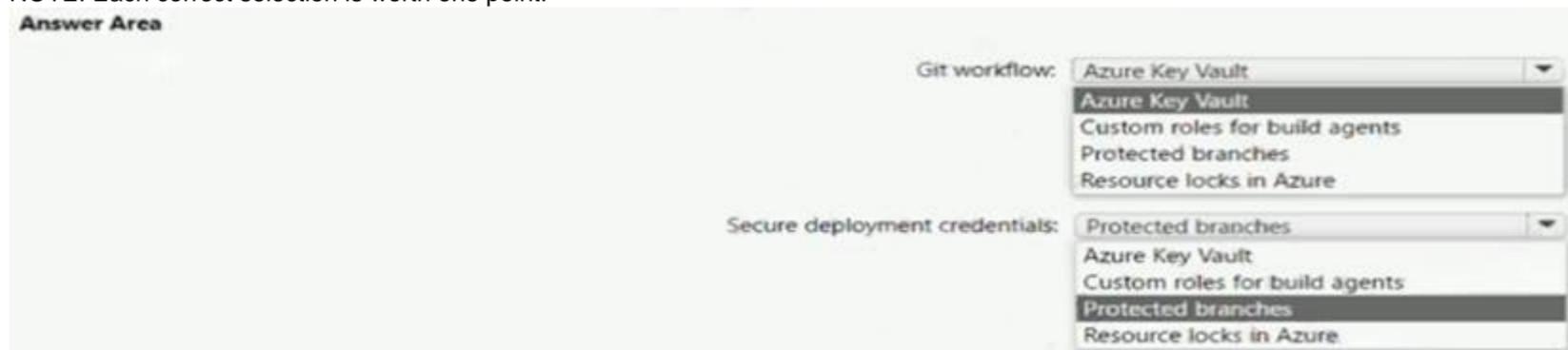
Explanation:

<https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory> <https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-acc>

NEW QUESTION 123

- (Exam Topic 3)

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CO) workflows. You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation for each stage? 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:



NEW QUESTION 128

- (Exam Topic 3)

You have an Azure SQL database named DB1 that contains customer information. A team of database administrators has full access to DB1. To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information. You need to design a security strategy for DB1. The solution must meet the following requirements:

- When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.
 - When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.
- What should you include in the design? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

For the database administrators: Always Encrypted

- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators: Row-level security (RLS)

- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

For the database administrators: Always Encrypted

- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators: Row-level security (RLS)

- Always Encrypted
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

NEW QUESTION 133

- (Exam Topic 3)

You are designing a security operations strategy based on the Zero Trust framework.

You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).

Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer, move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.

Actions	Answer Area
Establish ransomware recovery readiness.	
Implement disaster recovery.	
Establish visibility.	
Enable additional protection and detection controls.	
Enable automation.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Establish ransomware recovery readiness.	
Implement disaster recovery.	
Establish visibility.	Establish visibility.
Enable additional protection and detection controls.	Enable additional protection and detection controls.
Enable automation.	Enable automation.

NEW QUESTION 135

- (Exam Topic 3)

You plan to automate the development and deployment of a Nodejs-based app by using GitHub. You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

- Automate the generation of pull requests that remediate identified vulnerabilities.
- Automate vulnerability code scanning for public and private repositories.
- Minimize administrative effort.
- Minimize costs.

What should you recommend using? 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:

A close up of a text Description automatically generated

NEW QUESTION 138

- (Exam Topic 3)

You are designing a security operations strategy based on the Zero Trust framework.

You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts. What should you do?

- A. Enable built-in compliance policies in Azure Policy.
- B. Enable self-healing in Microsoft 365 Defender.
- C. Automate data classification.
- D. Create hunting queries in Microsoft 365 Defender.

Answer: C

NEW QUESTION 139

- (Exam Topic 3)

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface. What should you include in the recommendation?

- A. Azure Firewall Premium
- B. Azure Application Gateway Web Application Firewall (WAF)
- C. network security groups (NSGs)
- D. Azure Traffic Manager and application security groups

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection>

NEW QUESTION 141

- (Exam Topic 3)

You have 50 Azure subscriptions.

You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.

NOTE: Each correct selection is worth one point.

- A. Assign an initiative to a management group.
- B. Assign a policy to each subscription.
- C. Assign a policy to a management group.
- D. Assign an initiative to each subscription.
- E. Assign a blueprint to each subscription.
- F. Assign a blueprint to a management group.

Answer: AF

Explanation:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview> <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>
<https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001> <https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

NEW QUESTION 144

- (Exam Topic 3)

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 AllowShareKeyAccess property to false.
- C. Set the AllowBlobPublicAccess property to false.
- D. Configure automated key rotation.

Answer: A

Explanation:

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

NEW QUESTION 149

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SC-100 Practice Exam Features:

- * SC-100 Questions and Answers Updated Frequently
- * SC-100 Practice Questions Verified by Expert Senior Certified Staff
- * SC-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-100 Practice Test Here](#)