



Microsoft

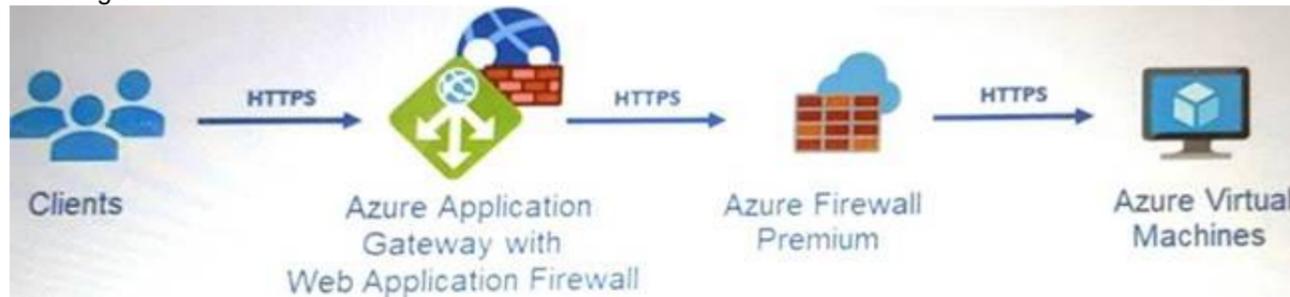
Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1

- (Exam Topic 3)

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-

- Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
- Use Defender for Cloud to review alerts from the virtual machines.

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

For WAF:

- The Azure Diagnostics extension
- Azure Network Watcher
- Data connectors
- Workflow automation

For the virtual machines:

- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- The Log Analytics agent
- Workflow automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

NEW QUESTION 2

- (Exam Topic 3)

Your company wants to optimize ransomware incident investigations.

You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.

Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Implement a comprehensive strategy to reduce the risk of privileged access compromise.
- Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.
- Assess the current situation and identify the scope.
- Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.
- Identify the compromise recovery process.

Answer Area

- Assess the current situation and identify the scope.
- Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.
- Identify the compromise recovery process.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- Implement a comprehensive strategy to reduce the risk of privileged access compromise.
- Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

Answer Area

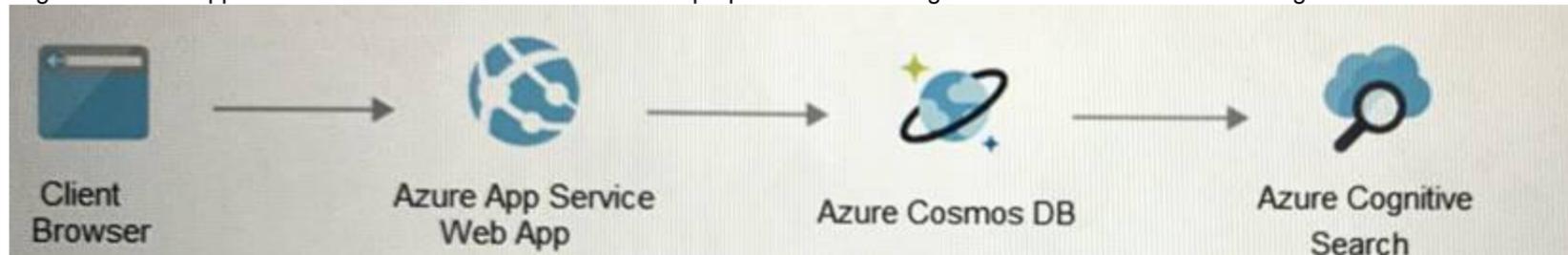
- Assess the current situation and identify the scope.
- Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.
- Identify the compromise recovery process.

NEW QUESTION 3

- (Exam Topic 3)

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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 Key Vault to store credentials.

- 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 4

- (Exam Topic 3)

You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements.
 What should you recommend as part of the landing zone deployment?

- A. service chaining
- B. local network gateways
- C. forced tunneling
- D. a VNet-to-VNet connection

Answer: A

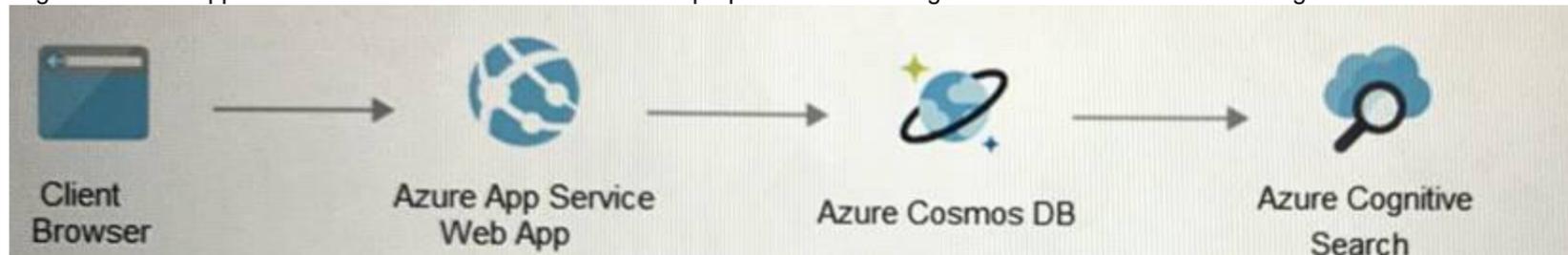
Explanation:

<https://docs.microsoft.com/en-us/learn/modules/configure-vnet-peering/5-determine-service-chaining-uses>

NEW QUESTION 5

- (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 Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

<https://www.varonis.com/blog/securing-access-azure-webapps>

NEW QUESTION 6

- (Exam Topic 3)

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 Registry
- B. Linux containers deployed to Azure Kubernetes Service (AKS)
- C. Windows containers deployed to Azure Container Registry
- D. Windows containers deployed to Azure Kubernetes Service (AKS)
- E. Linux containers deployed to Azure Container Instances

Answer: AC

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-sec> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabi>

NEW QUESTION 7

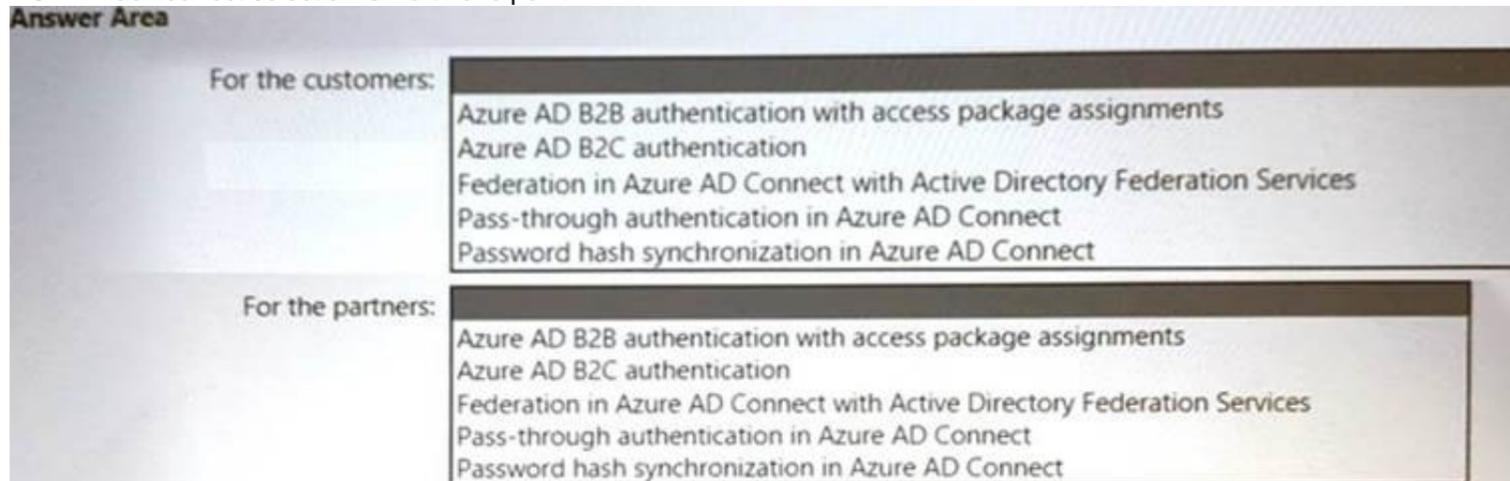
- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS). You need to recommend an identity security strategy that meets the following requirements:

- Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website
- Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components. 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

Box 1 --> <https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview>

Box 2 --> <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers>

NEW QUESTION 8

- (Exam Topic 3)

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. Microsoft Defender for Endpoint
- B. Windows Defender Device Guard
- C. protected folders
- D. Azure Files
- E. BitLocker Drive Encryption (BitLocker)

Answer: E

NEW QUESTION 9

- (Exam Topic 3)

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

Answer: AB

Explanation:

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

NEW QUESTION 10

- (Exam Topic 3)

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. a relying party trust in Active Directory Federation Services (AD FS)
- C. Azure AD Application Proxy
- D. Azure AD B2C

Answer: A

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 11

- (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 14

- (Exam Topic 3)

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel. You plan to integrate Microsoft Sentinel with Splunk.

You need to recommend a solution to send security events from Microsoft Sentinel to Splunk. What should you include in the recommendation?

- A. Azure Event Hubs
- B. Azure Data Factor
- C. a Microsoft Sentinel workbook
- D. a Microsoft Sentinel data connector

Answer: D

Explanation:

<https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-ev>

NEW QUESTION 18

- (Exam Topic 3)

Your company has an on-premises network and an Azure subscription.

The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.

You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.

You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.

What should you include in the recommendation?

- A. a private endpoint
- B. hybrid connections
- C. virtual network NAT gateway integration
- D. virtual network integration

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections>

NEW QUESTION 19

- (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 22

- (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?

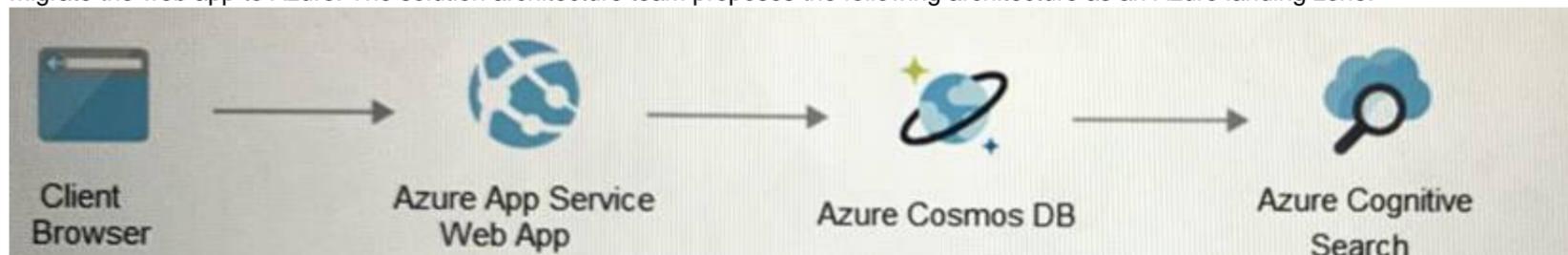
- A. From a Recovery Services vault generate a security PIN for critical operations.
- B. From Azure Backup, configure multi-user authorization by using Resource Guard.
- C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.
- D. From Azure AD Privileged Identity Management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

Answer: B

NEW QUESTION 23

- (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 creating private endpoints for the web app and the database layer. Does this meet the goal?

- A. Yes
- B. No

Answer: A

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.

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>

NEW QUESTION 28

- (Exam Topic 3)

Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

What should you recommend?

- A. Compliance Manager in Microsoft Purview
- B. Microsoft Defender for Cloud
- C. Microsoft Sentinel
- D. Microsoft Defender for Cloud Apps

Answer: D

NEW QUESTION 33

- (Exam Topic 3)

You are designing the encryption standards for data at rest for an Azure resource.

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 35

- (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

Automatically identify threats:

Enforce security settings:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Answer Area

Automatically identify threats:

Enforce security settings:

NEW QUESTION 39

- (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 43

- (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:

- Azure AD application
- Azure AD Application Proxy
- Azure Application Gateway
- A managed identity in Azure AD
- Microsoft Defender for App

To implement access requests for App1, use:

- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- An access review in Identity Governance
- Azure AD Conditional Access App Control
- 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 48

- (Exam Topic 3)

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud. You receive the following recommendations in Defender for Cloud

- Access to storage accounts with firewall and virtual network configurations should be restricted,
- Storage accounts should restrict network access using virtual network rules.
- Storage account should use a private link connection.
- Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations. What should you recommend?

- A. Azure Storage Analytics
- B. Azure Network Watcher
- C. Microsoft Sentinel
- D. Azure Policy

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept> <https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

NEW QUESTION 49

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

- A. insider risk management policies
- B. data loss prevention (DLP) policies
- C. sensitivity label policies
- D. retention policies

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

NEW QUESTION 50

- (Exam Topic 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 Defender for Cloud, review the Azure security baseline for audit report.
- B. From Defender for Cloud, review the secure score recommendations.
- C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
- D. From Defender for Cloud, enable Defender for Cloud plans.

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula>

NEW QUESTION 55

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

The company plans to deploy 45 mobile self-service kiosks that will run Windows 10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:

- Ensure that only authorized applications can run on the kiosks.
- Regularly harden the kiosks against new threats.

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

- A. Onboard the kiosks to Azure Monitor.
- B. Implement Privileged Access Workstation (PAW) for the kiosks.
- C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
- D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
- E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Answer: DE

Explanation:

(<https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerab>)

NEW QUESTION 58

- (Exam Topic 2)

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Security Assertion Markup Language (SAML)
- B. NTLMv2
- C. certificate-based authentication
- D. Kerberos

Answer: AD

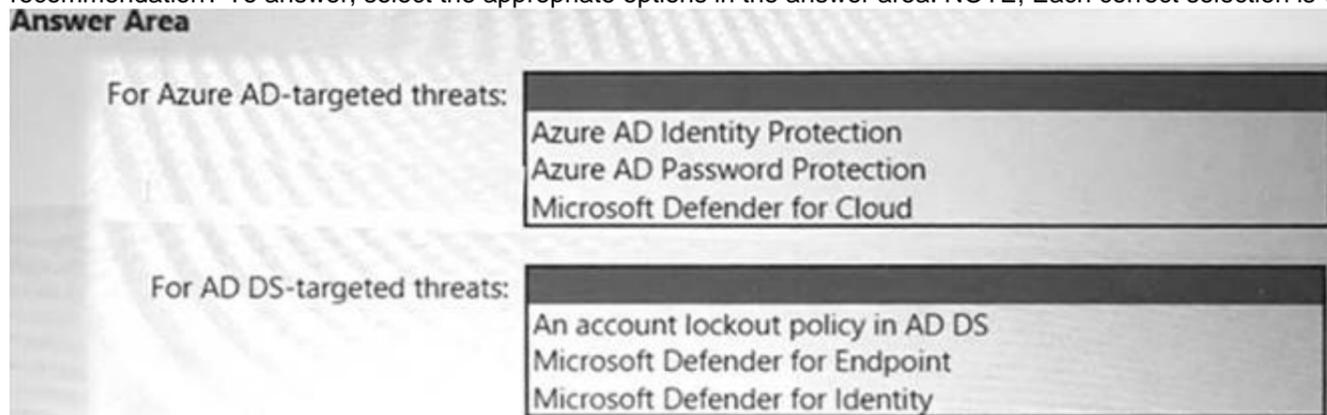
Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-o> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-w> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain>

NEW QUESTION 62

- (Exam Topic 2)

You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

* 1. Azure AD Identity Protection Brute Force Detection:

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

* 2. Defender for Identity

MDI can detect brute force attacks: ref:

<https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts#suspected-brute-force-at>

NEW QUESTION 67

- (Exam Topic 2)

You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements. What should you configure for each landing zone?

- A. Azure DDoS Protection Standard
- B. an Azure Private DNS zone
- C. Microsoft Defender for Cloud
- D. an ExpressRoute gateway

Answer: D

Explanation:

One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive. Given the landing zone requirements of

1) "Use a DNS namespace of litware.com"

2) "Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints"

NEW QUESTION 70

- (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

Segment Microsoft Sentinel workspaces by:

- Azure AD tenant
- Enterprise
- Region and Azure AD tenant

Integrate Azure subscriptions by using:

- Self-service sign-up user flows for Azure AD B2B
- Self-service sign-up user flows for Azure AD B2C
- The Azure Lighthouse subscription onboarding process

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 73

- (Exam Topic 1)

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

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

For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

NEW QUESTION 76

- (Exam Topic 1)

What should you create in Azure AD to meet the Contoso developer requirements?

Account type for the developers:

- A guest account in the contoso.onmicrosoft.com tenant
- A guest account in the fabrikam.onmicrosoft.com tenant
- A synced user account in the corp.fabrikam.com domain
- A user account in the fabrikam.onmicrosoft.com tenant

Component in Identity Governance:

- A connected organization
- An access package
- An access review
- An Azure AD role
- An Azure resource role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: A synced user account - Need to use a synced user account.

Box 2: An access review

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

NEW QUESTION 77

- (Exam Topic 1)

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

NEW QUESTION 79

- (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 81

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

- A. an Azure AD user account that has a password stored in Azure Key Vault
- B. a group managed service account (gMSA)
- C. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management(PIM)
- D. a managed identity in Azure

Answer: D

NEW QUESTION 84

- (Exam Topic 3)

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

Answer: A

Explanation:

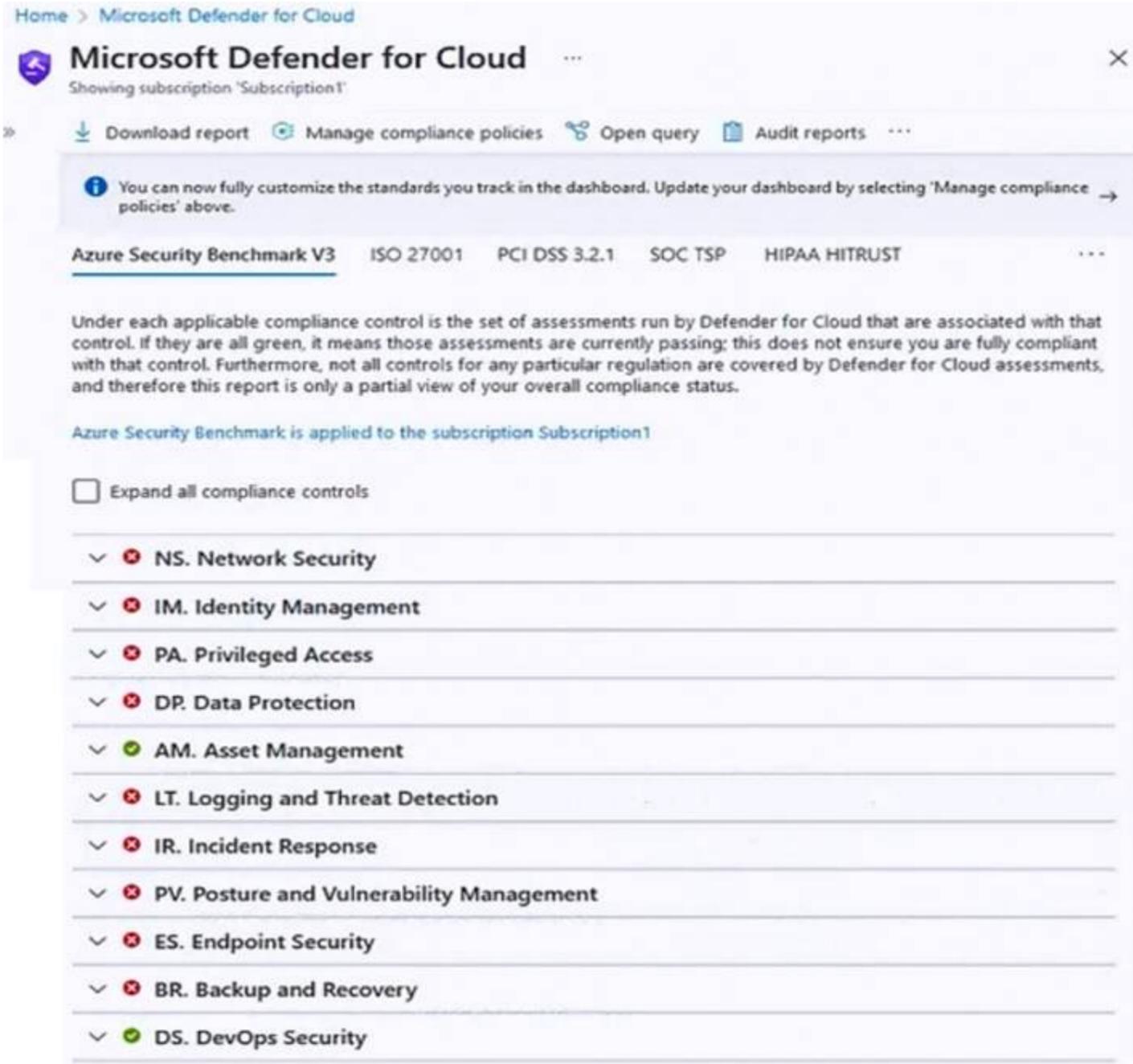
<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s>

NEW QUESTION 85

- (Exam Topic 3)

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

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.



You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

- A. Data Protection
- B. Incident Response
- C. Posture and Vulnerability Management
- D. Asset Management
- E. Endpoint Security

Answer: E

Explanation:
<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security>

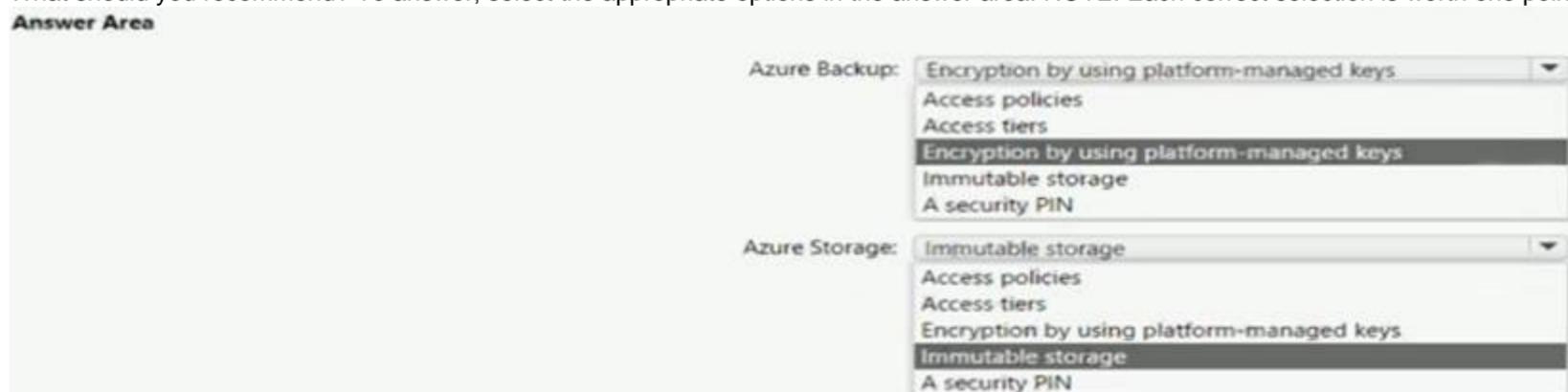
NEW QUESTION 87

- (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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 88

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscripits You need to evaluate the existing environment to increase the overall security posture for the following components:

- Windows 11 devices managed by Microsoft Intune
- Azure Storage accounts
- Azure virtual machines

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

Windows 11 devices:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure virtual machines:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure Storage accounts:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it). Selection 2: Microsoft Defender for Cloud.

Selection 3: Microsoft Defender for Cloud.

<https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-sec>

NEW QUESTION 93

- (Exam Topic 3)

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender

You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender

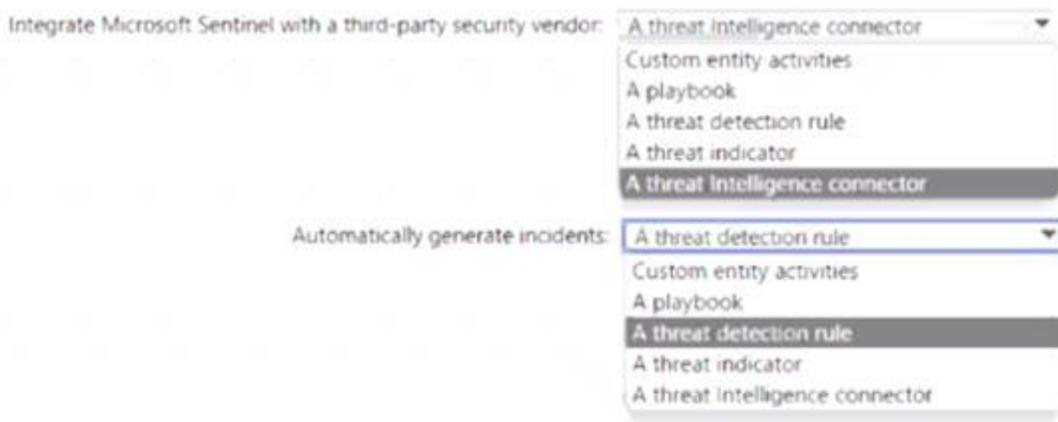
You need to recommend a solution to meet the following requirements:

- Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
- Automatically generate incidents when the IP address of a command-and control server is detected in the events

What should you configure in Microsoft Sentinel to meet 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 97

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.

The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network. You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

- Prevent the remote users from accessing any other resources on the network.
- Support Azure Active Directory (Azure AD) Conditional Access.
- Simplify the end-user experience.

What should you include in the recommendation?

- A. Azure AD Application Proxy
- B. Azure Virtual WAN
- C. Microsoft Tunnel
- D. web content filtering in Microsoft Defender for Endpoint

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore>

NEW QUESTION 100

- (Exam Topic 3)

You have an Active Directory Domain Services (AD DS) domain that contains a virtual desktop infrastructure (VDI). The VDI uses non-persistent images and cloned virtual machine templates. VDI devices are members of the domain.

You have an Azure subscription that contains an Azure Virtual Desktop environment. The environment contains host pools that use a custom golden image. All the Azure Virtual Desktop deployments are members of a single Azure Active Directory Domain Services (Azure AD DS) domain.

You need to recommend a solution to deploy Microsoft Defender for Endpoint to the hosts. The solution must meet the following requirements:

- Ensure that the hosts are onboarded to Defender for Endpoint during the first startup sequence.
- Ensure that the Microsoft Defender 365 portal contains a single entry for each deployed VDI host.
- Minimize administrative effort.

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

Answer Area

For the VDI:

- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.**

For Azure Virtual Desktop:

- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.**

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Answer Area

For the VDI:

- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.**

For Azure Virtual Desktop:

- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.**

NEW QUESTION 101

- (Exam Topic 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 Defender for Cloud, review the secure score recommendations.
- 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 Defender for Cloud, add a regulatory compliance standard.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula>

NEW QUESTION 103

- (Exam Topic 3)

Your company has an office in Seattle.

The company has two Azure virtual machine scale sets hosted on different virtual networks. The company plans to contract developers in India.

You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:

- Prevent exposing the public IP addresses of the virtual machines.
- Provide the ability to connect without using a VPN.
- Minimize costs.

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

- A. Deploy Azure Bastion to one virtual network.
- B. Deploy Azure Bastion to each virtual network.
- C. Enable just-in-time VM access on the virtual machines.
- D. Create a hub and spoke network by using virtual network peering.
- E. Create NAT rules and network rules in Azure Firewall.

Answer: AD

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion>

NEW QUESTION 107

- (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 108

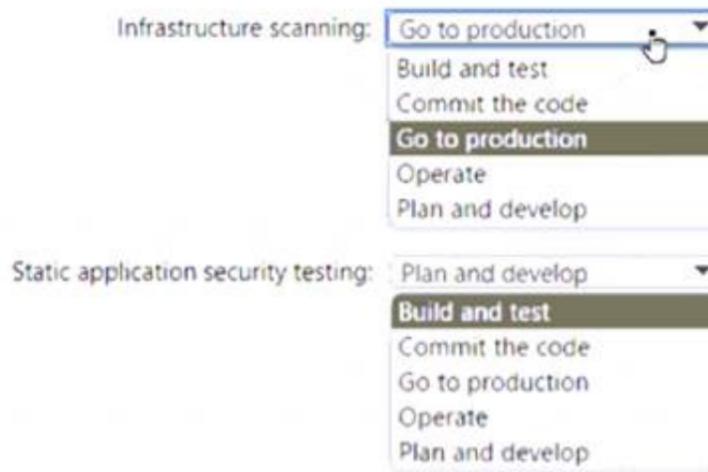
- (Exam Topic 3)

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines

You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines. What should 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:

Answer Area



NEW QUESTION 109

- (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 D81. 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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Answer Area



NEW QUESTION 112

- (Exam Topic 3)

Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app. You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection. What should you include in the recommendation?

- A. interactive application security testing (IAST)
- B. static application security testing (SAST)
- C. runtime application self-protection (RASP)
- D. dynamic application security testing (DAST)

Answer: D

Explanation:
<https://docs.microsoft.com/en-us/azure/security/develop/secure-develop#test-your-application-in-an-operating-st>

NEW QUESTION 116

- (Exam Topic 3)

Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Answer: C

Explanation:
<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

<https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion>

NEW QUESTION 118

- (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 120

- (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 125

- (Exam Topic 3)

You are designing an auditing solution for Azure landing zones that will contain the following components:

- SQL audit logs for Azure SQL databases
- Windows Security logs from Azure virtual machines
- Azure App Service audit logs from App Service web apps

You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:

- Log all privileged access.
- Retain logs for at least 365 days.
- Minimize costs.

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



For the SQL audit logs:
 A Log Analytics workspace
 Azure Application Insights
 For the Security logs: Microsoft Defender for SQL
 Microsoft Sentinel

For the Security logs:
 A Log Analytics workspace
 Application Insights
 For the App Service audit logs: Microsoft Defender for servers
 Microsoft Sentinel

For the App Service audit logs:
 A Log Analytics workspace
 Application Insights
 Microsoft Defender for App Service
 Microsoft Sentinel

NEW QUESTION 128

- (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 130

- (Exam Topic 3)

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices. What is the first step in the recovery plan?

- A. Disable Microsoft OneDrive sync and Exchange ActiveSync.
- B. Recover files to a cleaned computer or device.
- C. Contact law enforcement.
- D. From Microsoft Defender for Endpoint perform a security scan.

Answer: A

NEW QUESTION 132

- (Exam Topic 3)

You have the following on-premises servers that run Windows Server:

- Two domain controllers in an Active Directory Domain Services (AD DS) domain
- Two application servers named Server1 and Server2 that run ASP.NET web apps
- A VPN server named Server3 that authenticates by using RADIUS and AD DS. End users use a VPN to access the web apps over the internet.

You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

What should you include in the recommendation?

- A. Configure connectors and rules in Microsoft Defender for Cloud Apps.
- B. Configure web protection in Microsoft Defender for Endpoint.
- C. Publish the web apps by using Azure AD Application Proxy.
- D. Configure the VPN to use Azure AD authentication.

Answer: C

NEW QUESTION 133

.....

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](#)