

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)

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

- Azure IoT Edge devices
- AWS EC2 instances

Which services 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 IoT Edge devices:	<div><div></div>Azure Arc</div>
For the AWS EC2 instances:	<div><div></div>Microsoft Defender for Cloud</div> <div><div></div>Microsoft Defender for Cloud Apps</div> <div><div></div>Microsoft Defender for Endpoint</div> <div><div></div>Microsoft Defender for IoT</div>
For the AWS EC2 instances:	<div><div></div>Azure Arc only</div> <div><div></div>Microsoft Defender for Cloud and Azure Arc</div> <div><div></div>Microsoft Defender for Cloud Apps only</div> <div><div></div>Microsoft Defender for Cloud only</div> <div><div></div>Microsoft Defender for Endpoint and Azure Arc</div> <div><div></div>Microsoft Defender for Endpoint only</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings> <https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations>

NEW QUESTION 3

- (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 onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 4

- (Exam Topic 3)

Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure. You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.
What should you include in the recommendation?

- A. Use geo-redundant storage (GRS).
- B. Use customer-managed keys (CMKs) for encryption.
- C. Require PINs to disable backups.
- D. Implement Azure Site Recovery replication.

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#azure>

NEW QUESTION 5

- (Exam Topic 3)

You have an operational model based on the Microsoft Cloud Adoption framework for Azure.
You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, database, files, and storage accounts.
What should you include in the recommendation?

- A. security baselines in the Microsoft Cloud Security Benchmark
- B. modern access control
- C. business resilience
- D. network isolation

Answer: A

NEW QUESTION 6

- (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

<

>

- 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

1 Assess the current situation and identify the scope.

2 Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.

3 Identify the compromise recovery process.

<

>

NEW QUESTION 7

- (Exam Topic 3)

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD)
The customer plans to obtain an Azure subscription and provision several Azure resources. You need to evaluate the customer's security environment.
What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

- A. role-based authorization
- B. Azure AD Privileged Identity Management (PIM)
- C. resource-based authorization
- D. Azure AD Multi-Factor Authentication

Answer: D

Explanation:

(<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>) <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing?rtc=1>

NEW QUESTION 8

- (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

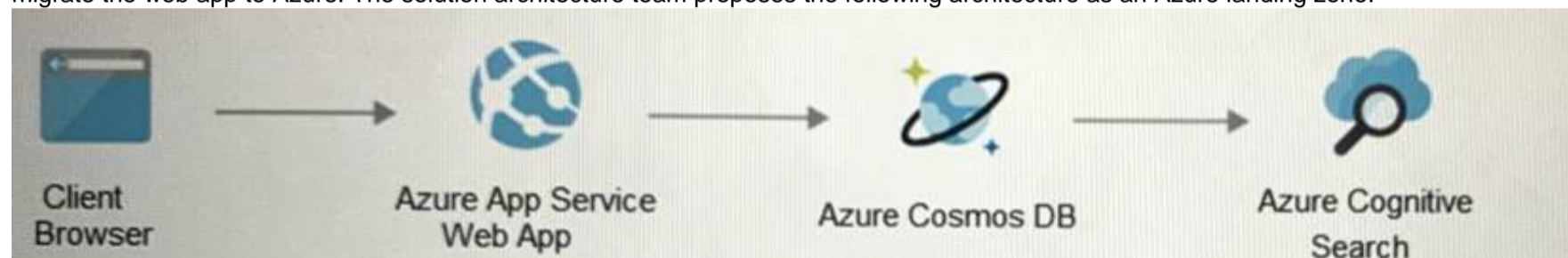
Explanation:

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

NEW QUESTION 9

- (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 10

- (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 10

- (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 15

- (Exam Topic 3)

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions. You are evaluating the security posture of the customer.

You discover that the AKS resources are excluded from the secure score recommendations. You need to produce accurate recommendations and update the secure score.

Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Configure auto provisioning.
- B. Assign regulatory compliance policies.
- C. Review the inventory.
- D. Add a workflow automation.
- E. Enable Defender plans.

Answer: AE

Explanation:

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

NEW QUESTION 16

- (Exam Topic 3)

You are designing the security standards for a new Azure environment.

You need to design a privileged identity strategy based on the Zero Trust model. Which framework should you follow to create the design?

- A. Enhanced Security Admin Environment (ESAE)
- B. Microsoft Security Development Lifecycle (SDL)
- C. Rapid Modernization Plan (RaMP)
- D. Microsoft Operational Security Assurance (OSA)

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan> This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

NEW QUESTION 17

- (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 20

- (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 22

- (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 27

- (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

Developer: Specialized security
 Enterprise security
 Privileged security
 Specialized security

Standard user: Enterprise security
 Enterprise security
 Privileged security
 Specialized security

IT administrator: Privileged security
 Enterprise security
 Privileged security
 Specialized security

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Developer: Specialized security
 Enterprise security
 Privileged security
 Specialized security

Standard user: Enterprise security
 Enterprise security
 Privileged security
 Specialized security

IT administrator: Privileged security
 Enterprise security
 Privileged security
 Specialized security

NEW QUESTION 32

- (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. Configure Azure Active Directory (Azure AD) Conditional Access policies.
- B. Use the Azure Monitor agent with the multi-homing configuration.
- C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
- D. Create a custom collector that uses the Log Analytics agent.

Answer: BC

NEW QUESTION 35

- (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 36

- (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 41

- (Exam Topic 3)

You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

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

Data security:

<input type="checkbox"/> Access keys stored in Azure Key Vault <input type="checkbox"/> Automation Contributor built-in role <input type="checkbox"/> Azure Private Link with network service tags <input type="checkbox"/> Azure Web Application Firewall rules with network service tags

Network access control:

<input type="checkbox"/> Access keys stored in Azure Key Vault <input type="checkbox"/> Automation Contributor built-in role <input type="checkbox"/> Azure Private Link with network service tags <input type="checkbox"/> Azure Web Application Firewall rules with network service tags

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Data Security = Access Keys stored in Azure Key Vault

Network access control = Azure Private Link with network service tags

<https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security>

NEW QUESTION 43

- (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 m near-real-lime (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 47

- (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 48

- (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 49

- (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 52

- (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 54

- (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 57

- (Exam Topic 2)

You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity 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

For the delegated management of users and groups, use:

- AD DS organizational units
- Azure AD administrative units
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

- Enable password hash synchronization in the Azure AD Connect deployment
- Enable Security defaults in the Azure AD tenant of Litware
- Replace pass-through authentication with Active Directory Federation Services

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

For the delegated management of users and groups, use:

- AD DS organizational units
- Azure AD administrative units
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

- Enable password hash synchronization in the Azure AD Connect deployment
- Enable Security defaults in the Azure AD tenant of Litware
- Replace pass-through authentication with Active Directory Federation Services

NEW QUESTION 60

- (Exam Topic 2)

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone 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

For connectivity from App Service web apps to virtual machines, use:

- Private endpoints
- Service endpoints
- Virtual network integration

For connectivity from virtual machines to App Service web apps, use:

- Private endpoints
- Service endpoints
- Virtual network integration

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Virtual Network Integration - correct

Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network.

Box 2: Private Endpoints. - correct

You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.

NEW QUESTION 62

- (Exam Topic 1)

You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?

- A. Azure Key Vault
- B. GitHub Advanced Security
- C. Application Insights in Azure Monitor
- D. Azure DevTest Labs

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/introduction-github-advanced-security/2-what-is-github-advanc>

NEW QUESTION 66

- (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 69

- (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 synched 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 71

- (Exam Topic 1)

You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

- A. an Azure Bastion host
- B. a network security group (NSG)
- C. just-in-time (JIT) VM access
- D. Azure Virtual Desktop

Answer: A

Explanation:

The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image."
<https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image>

NEW QUESTION 75

- (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:	<input type="checkbox"/> A NAT gateway <input type="checkbox"/> A network security group <input type="checkbox"/> A private endpoint <input type="checkbox"/> A service endpoint
The app services permission for ClaimsApp must be assigned to ClaimsDB:	<input type="checkbox"/> A custom role-based access control (RBAC) role <input type="checkbox"/> A managed identity <input type="checkbox"/> An access package <input type="checkbox"/> 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:	<input type="checkbox"/> A NAT gateway <input checked="" type="checkbox"/> A network security group <input checked="" type="checkbox"/> A private endpoint <input type="checkbox"/> A service endpoint
The app services permission for ClaimsApp must be assigned to ClaimsDB:	<input type="checkbox"/> A custom role-based access control (RBAC) role <input checked="" type="checkbox"/> A managed identity <input type="checkbox"/> An access package <input type="checkbox"/> Azure AD Privileged Identity Management (PIM)

NEW QUESTION 80

- (Exam Topic 3)

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).

You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment

What should you include during the application design phase?

- A. static application security testing (SAST) by using SonarQube
- B. dynamic application security testing (DAST) by using Veracode
- C. threat modeling by using the Microsoft Threat Modeling Tool
- D. software decomposition by using Microsoft Visual Studio Enterprise

Answer: C

Explanation:

<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

NEW QUESTION 84

- (Exam Topic 3)

Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool. Which type of diagram should you create?

- A. data flow
- B. system flow
- C. process flow
- D. network flow

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram> <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started?source=recommen>

NEW QUESTION 88

- (Exam Topic 3)

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware. The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Microsoft Defender for Endpoint reports the endpoints as compliant.
- B. Microsoft Intune reports the endpoints as compliant.
- C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
- D. The client access tokens are refreshed.

Answer: CD

Explanation:

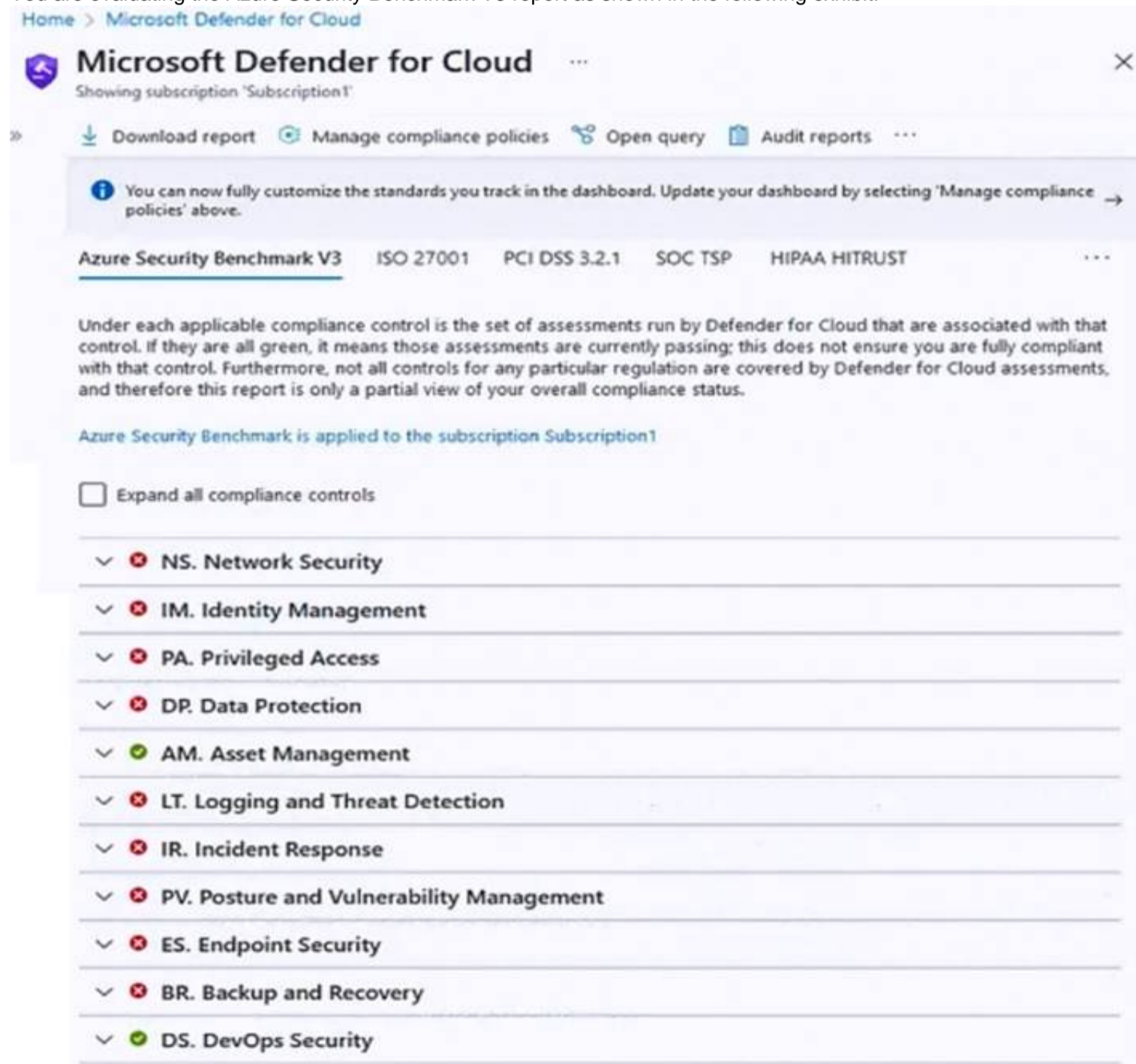
<https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust> <https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens>

NEW QUESTION 89

- (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.



Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud ...

Showing subscription 'Subscription1'

» Download report Manage compliance policies Open query Audit reports ...

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Azure Security Benchmark V3 ISO 27001 PCI DSS 3.2.1 SOC TSP HIPAA HITRUST ...

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription Subscription1

☒ Expand all compliance controls

- ▼ **NS. Network Security**
- ▼ **IM. Identity Management**
- ▼ **PA. Privileged Access**
- ▼ **DP. Data Protection**
- ▼ **AM. Asset Management**
- ▼ **LT. Logging and Threat Detection**
- ▼ **IR. Incident Response**
- ▼ **PV. Posture and Vulnerability Management**
- ▼ **ES. Endpoint Security**
- ▼ **BR. Backup and Recovery**
- ▼ **DS. DevOps Security**

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 92

- (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 96

- (Exam Topic 3)

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs. What should you include in the recommendation?

- A. Microsoft 365 Defender
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Cloud Apps
- D. Microsoft Sentinel

Answer: D

NEW QUESTION 100

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

- A. Microsoft Defender for Cloud Apps
- B. insider risk management
- C. Microsoft Information Protection
- D. Azure Purview

Answer: C

Explanation:

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

You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as Salesforce, Box, or Dropbox, even if the third-party app or service does not read or support sensitivity labels.

NEW QUESTION 102

- (Exam Topic 3)

Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.

What should you include in the recommendation?

- A. custom roles in Azure Pipelines
- B. branch policies in Azure Repos
- C. Azure policies
- D. custom Azure roles

Answer: B

NEW QUESTION 105

- (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 to allow traffic from the backend IP address of the Front Door instance.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 106

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure.

The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.

The company's security policy prevents the use of personal devices for accessing company data and applications.

You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.

What should you include in the recommendation?

- A. Migrate the on-premises applications to cloud-based applications.
- B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
- C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
- D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop> <https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide> <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-c>

NEW QUESTION 107

- (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

Manage NSG rules by using: Azure Bastion
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: Azure Bastion
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 112

- (Exam Topic 3)

For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management What should you include in the recommendation?

- A. device registrations in Azure AD
- B. application registrations m Azure AD
- C. Azure service principals with certificate credentials
- D. Azure service principals with usernames and passwords
- E. managed identities in Azure

Answer: E

NEW QUESTION 114

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services {AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices. You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised. What should you include in the recommendation?

- A. Local Administrator Password Solution (LAPS)
- B. Privileged Access Workstations (PAWs)
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure AD identity Protection

Answer: A

NEW QUESTION 117

- (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 122

- (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 126

- (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

Infrastructure scanning: Go to production

- Build and test
- Commit the code
- Go to production**
- Operate
- Plan and develop

Static application security testing: Plan and develop

- Build and test**
- Commit the code
- Go to production
- Operate
- Plan and develop

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Infrastructure scanning:

Go to production

Build and test

Commit the code

Go to production

Operate

Plan and develop

Static application security testing:

Plan and develop

Build and test

Commit the code

Go to production

Operate

Plan and develop

NEW QUESTION 127

- (Exam Topic 3)
You have a hybrid cloud infrastructure.
You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network.	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

App1:

Azure AD B2B authentication with Conditional Access

Azure AD B2C custom policies with Conditional Access

Azure Application Gateway Web Application Firewall policies

Azure Firewall

Azure VPN Gateway with network security group rules

Azure VPN Point-to-Site connections

App2:

Azure AD B2B authentication with Conditional Access

Azure AD B2C custom policies with Conditional Access

Azure Application Gateway Web Application Firewall policies

Azure Firewall

Azure VPN Gateway with network security group rules

Azure VPN Point-to-Site connections

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence

NEW QUESTION 131

- (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.

Answer Area

Git workflow:

Azure Key Vault

Azure Key Vault

Custom roles for build agents

Protected branches

Resource locks in Azure

Secure deployment credentials:

Protected branches

Azure Key Vault

Custom roles for build agents

Protected branches

Resource locks in Azure

- A. Mastered
- B. Not Mastered

Answer: A

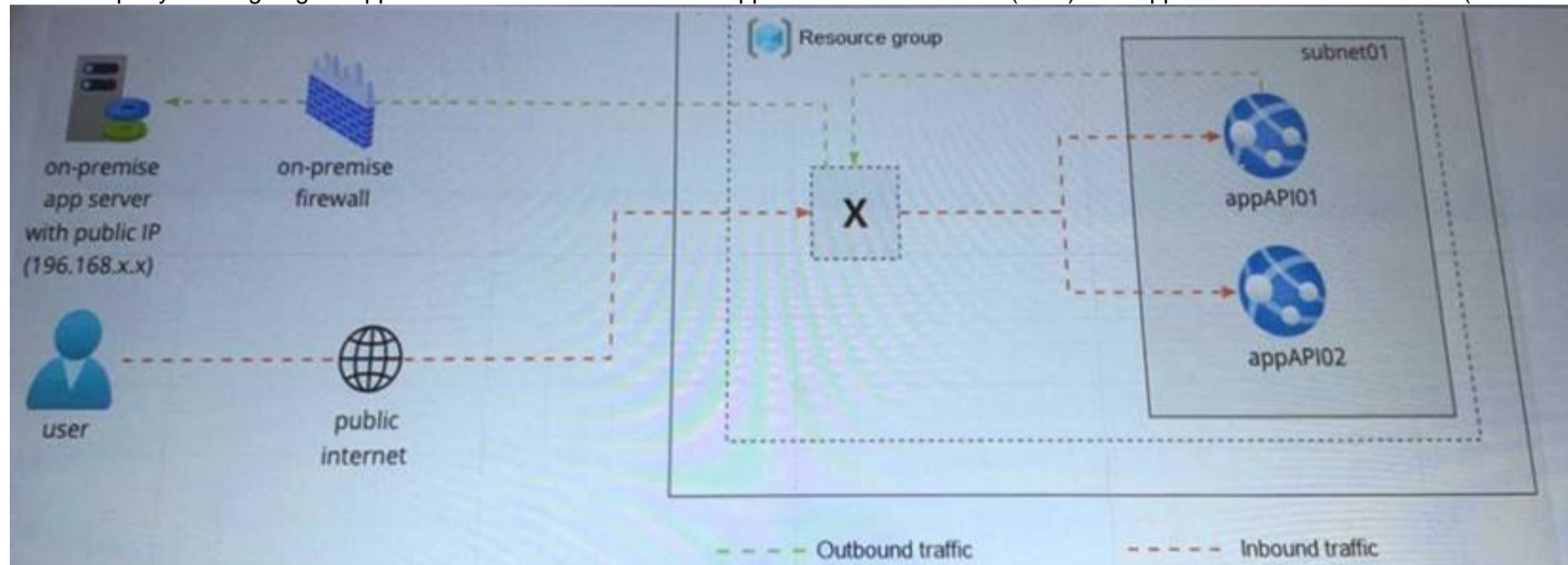
Explanation:



NEW QUESTION 136

- (Exam Topic 3)

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

- A. Azure Traffic Manager with priority traffic-routing methods
- B. Azure Application Gateway v2 with user-defined routes (UDRs).
- C. Azure Front Door with Azure Web Application Firewall (WAF)
- D. Azure Firewall with policy rule sets

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview>

NEW QUESTION 141

- (Exam Topic 3)

You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts. You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts. Which two configurations should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Enable Microsoft Defender for Cosmos DB.
- B. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.
- C. Disable local authentication for Azure Cosmos DB.
- D. Enable Microsoft Defender for Identity.
- E. Send the Azure Cosmos DB logs to a Log Analytics workspace.

Answer: BC

Explanation:

<https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs>

NEW QUESTION 144

.....

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](#)