

Exam Questions SC-100

Microsoft Cybersecurity Architect

<https://www.2passeasy.com/dumps/SC-100/>



NEW QUESTION 1

- (Exam Topic 3)

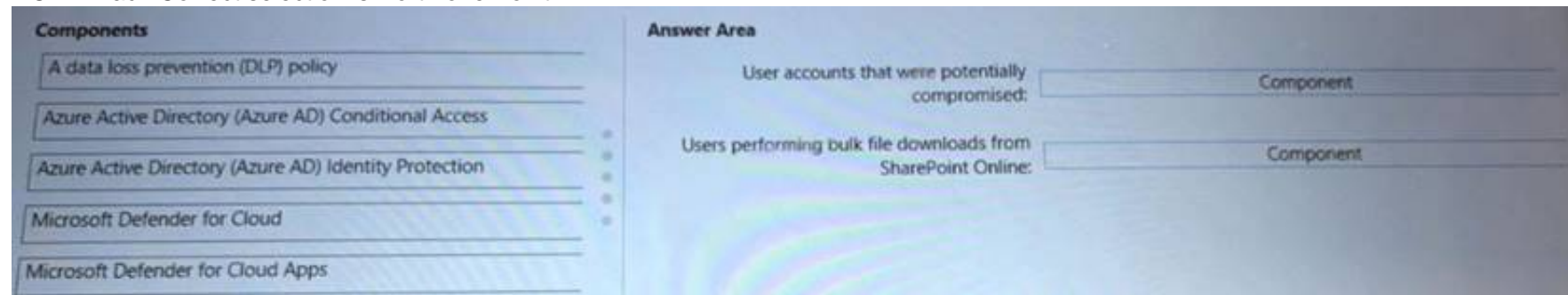
You have a Microsoft 365 subscription

You need to recommend a security solution to monitor the following activities:

- User accounts that were potentially compromised
- Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks> <https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exf> <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users>

NEW QUESTION 2

- (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 3

- (Exam Topic 3)

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment. You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. data, compliance, and governance
- B. user access and productivity
- C. infrastructure and development
- D. modern security operations
- E. operational technology (OT) and IoT

Answer: ABD

NEW QUESTION 4

- (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 5

- (Exam Topic 3)

You have a Microsoft 365 subscription.

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

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

- A. Microsoft Defender for Cloud Apps
- B. Azure AD Application Proxy
- C. Azure Data Catalog
- D. Azure AD Conditional Access
- E. Microsoft Purview Information Protection

Answer: AD

NEW QUESTION 6

- (Exam Topic 3)

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 7

- (Exam Topic 3)

You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

- A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
- A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

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

Answer Area

Deleted backups:	<div>Soft delete of backups</div> <div>A security PIN for critical operations</div> <div>Encryption by using a customer-managed key</div> <div>Multi-user authorization by using Resource Guard</div> <div>Soft delete of backups</div>
Disabled backups:	<div>Multi-user authorization by using Resource Guard</div> <div>A security PIN for critical operations</div> <div>Encryption by using a customer-managed key</div> <div>Multi-user authorization by using Resource Guard</div> <div>Soft delete of backups</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

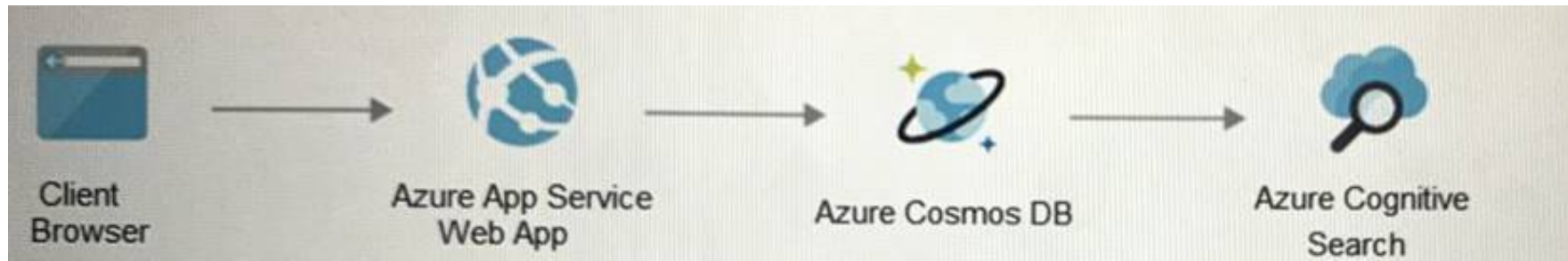
Answer Area

Deleted backups:	<div>Soft delete of backups</div> <div>A security PIN for critical operations</div> <div>Encryption by using a customer-managed key</div> <div>Multi-user authorization by using Resource Guard</div> <div>Soft delete of backups</div>
Disabled backups:	<div>Multi-user authorization by using Resource Guard</div> <div>A security PIN for critical operations</div> <div>Encryption by using a customer-managed key</div> <div>Multi-user authorization by using Resource Guard</div> <div>Soft delete of backups</div>

NEW QUESTION 8

- (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 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 9

- (Exam Topic 3)

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

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

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

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

Answer: CD

Explanation:

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

NEW QUESTION 10

- (Exam Topic 3)

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure.

You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure.

What should you use to start the threat modeling process?

- A. the STRIDE model
- B. the DREAD model
- C. OWASP threat modeling

Answer: C

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 12

- (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 13

- (Exam Topic 3)

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure. During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point

Answer Area

Threat modeling:

Build and test

Commit the code

Go to production

Operate

Plan and develop

Actionable intelligence:

Operate

Build and test

Commit the code

Go to production

Operate

Plan and develop

Dynamic application security testing (DAST):

Build and test

Build and test

Commit the code

Go to production

Operate

Plan and develop

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Threat modeling:

Build and test

Commit the code

Go to production

Operate

Plan and develop

Actionable intelligence:

Operate

Build and test

Commit the code

Go to production

Operate

Plan and develop

Dynamic application security testing (DAST):

Build and test

Build and test

Commit the code

Go to production

Operate

Plan and develop

NEW QUESTION 18

- (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 retying party trust in Active Directory Federation Services (AD FS)
- C. Azure AD Application Proxy
- D. Azure AD B2C

Answer: A

NEW QUESTION 23

- (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 27

- (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 30

- (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 31

- (Exam Topic 3)

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

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

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

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

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

Answer Area

DLP:	<div><div>Microsoft Purview</div><div>Azure Data Catalog</div><div>Azure Data Explorer</div><div>Microsoft Purview</div></div>
UEBA:	<div><div>Azure AD Identity Protection</div><div>Azure AD Identity Protection</div><div>Microsoft Defender for Identity</div><div>Microsoft Entra Verified ID</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

DLP:

UEBA:

NEW QUESTION 36

- (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 39

- (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 40

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events. What should you recommend using in Microsoft Sentinel?

- A. playbooks
- B. workbooks
- C. notebooks
- D. threat intelligence

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview>

NEW QUESTION 45

- (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.

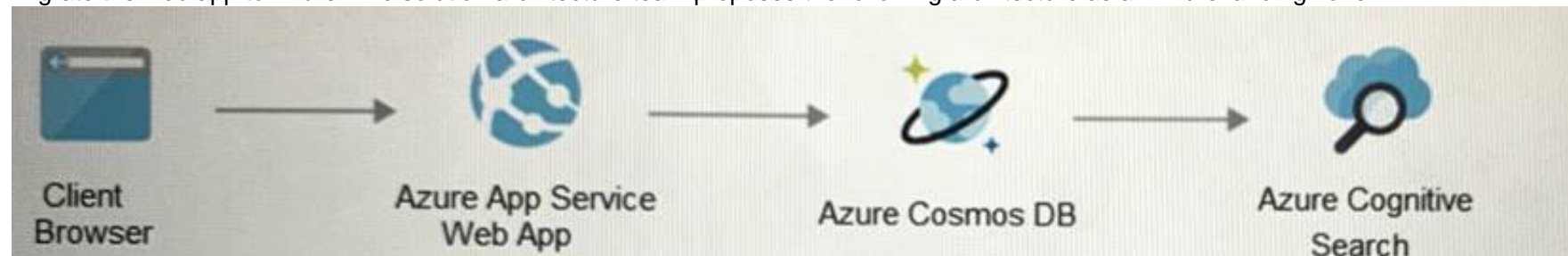
D. Create a custom collector that uses the Log Analytics agent.

Answer: BC

NEW QUESTION 49

- (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 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 51

- (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 56

- (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 57

- (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:

- Microsoft Defender for Cloud
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Enforce security settings:

- Microsoft Sentinel
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Automatically identify threats:

- Microsoft Defender for Cloud
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Enforce security settings:

- Microsoft Sentinel
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

NEW QUESTION 61

- (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 66

- (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 69

- (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 71

- (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 74

- (Exam Topic 2)

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

Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

NEW QUESTION 75

- (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 76

- (Exam Topic 2)

You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business 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

Evaluate regulatory compliance of cloud resources by assigning:

- Azure Policy definitions to management groups
- Azure Policy initiatives to management groups
- Azure Policy initiatives to subscriptions

Evaluate regulatory compliance of on-premises resources by using:

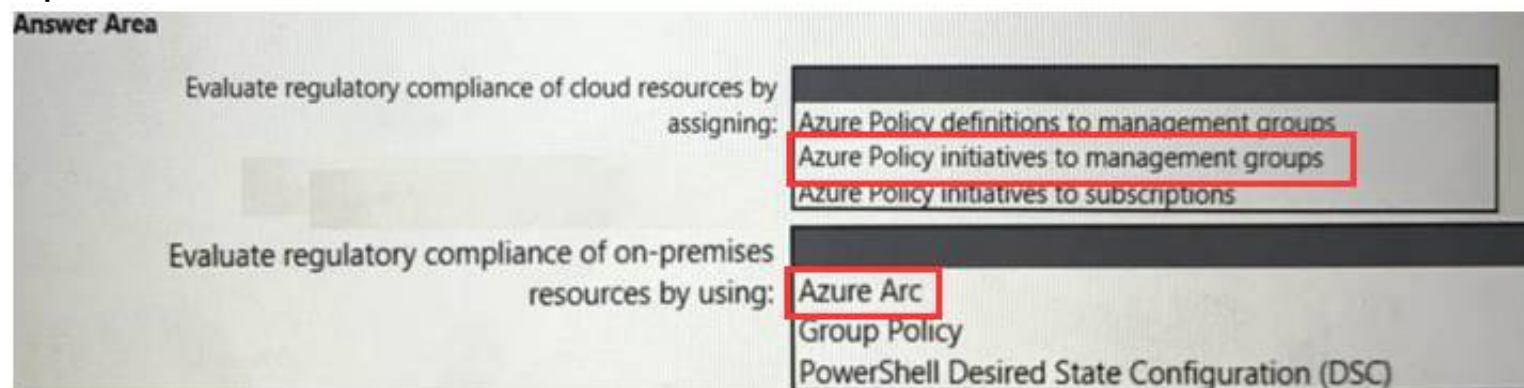
- Azure Arc
- Group Policy
- PowerShell Desired State Configuration (DSC)

- A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 81

- (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:

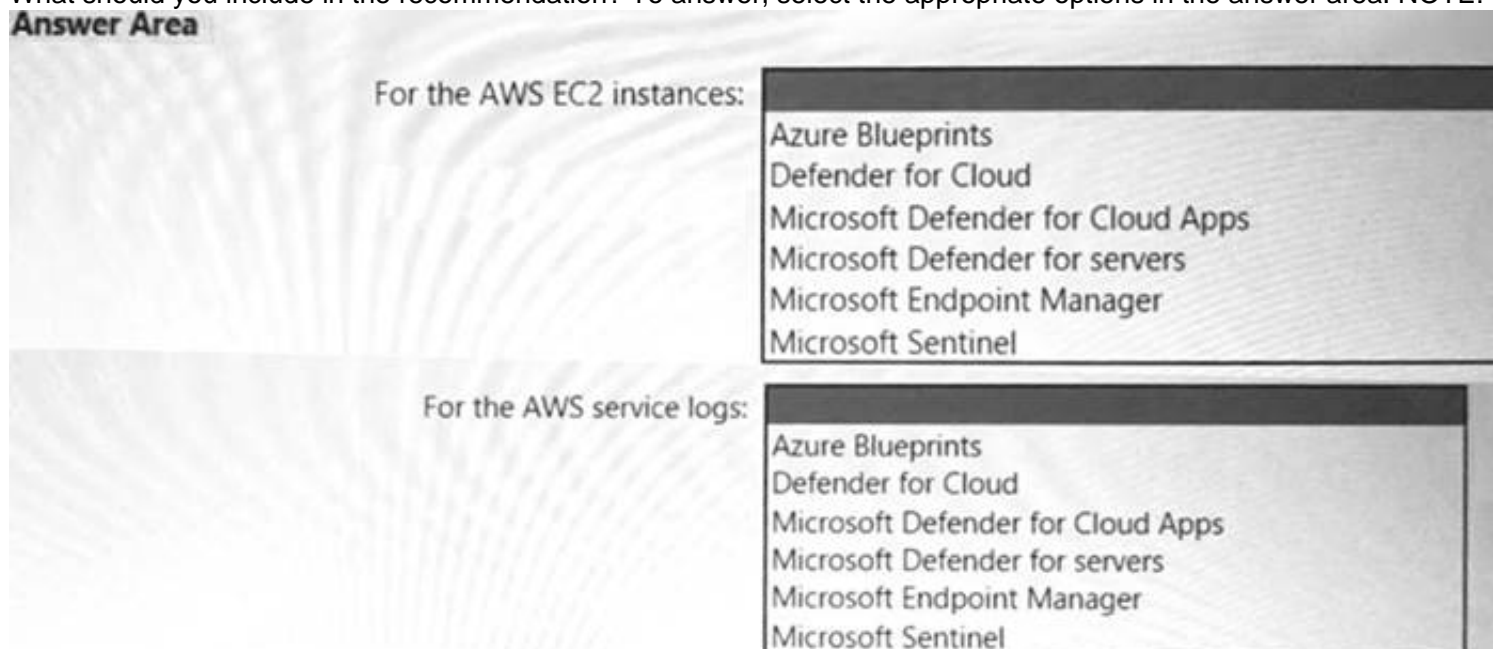
<https://docs.microsoft.com/en-us/learn/modules/introduction-github-advanced-security/2-what-is-github-advanc>

NEW QUESTION 86

- (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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 87

- (Exam Topic 1)

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

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

Answer: AC

Explanation:

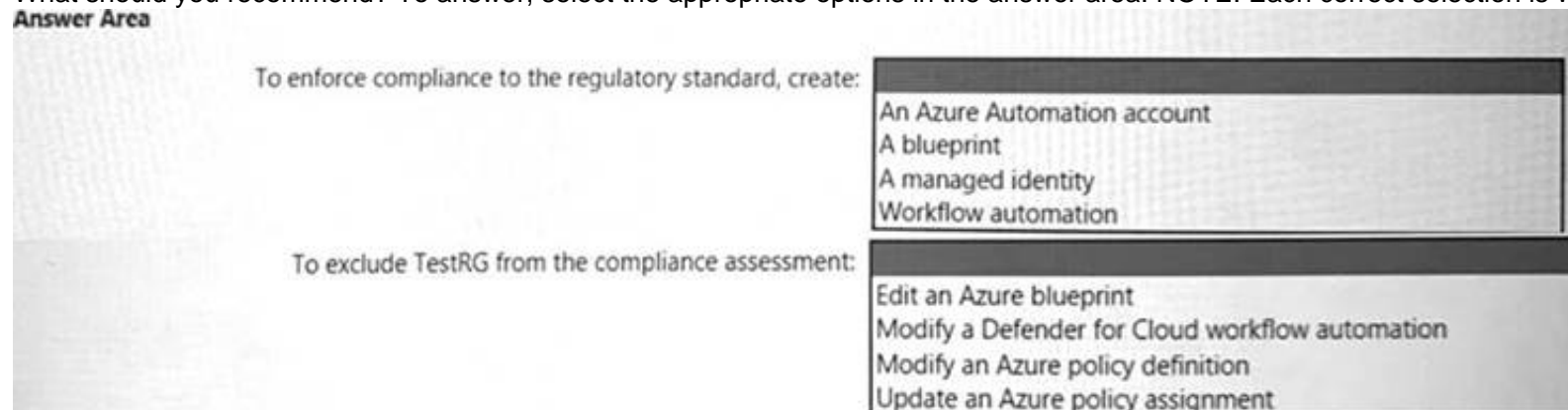
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365->

NEW QUESTION 92

- (Exam Topic 1)

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

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

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

while it is in policy assignment

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

NEW QUESTION 97

- (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 102

- (Exam Topic 1)

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements. What should you include in the recommendation?

- A. Transparent Data Encryption (TDE)
- B. Always Encrypted
- C. row-level security (RLS)
- D. dynamic data masking
- E. data classification

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-encl>

NEW QUESTION 106

- (Exam Topic 1)

You need to recommend a solution to meet the security requirements for the InfraSec group. What should you use to delegate the access?

- A. a subscription
- B. a custom role-based access control (RBAC) role
- C. a resource group
- D. a management group

Answer: B

NEW QUESTION 107

- (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 configuring gateway-required virtual network integration. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 112

- (Exam Topic 3)

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

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

Answer: AC

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management>

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

NEW QUESTION 117

- (Exam Topic 3)

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:

- Computers that run either Windows 10 or Windows 11
- Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored. What should you include in the recommendation?

- A. eDiscovery
- B. retention policies
- C. Compliance Manager
- D. Microsoft Information Protection

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection> <https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide>

NEW QUESTION 121

- (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 126

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically. What should you use?

- A. the regulatory compliance dashboard in Defender for Cloud
- B. Azure Policy
- C. Azure Blueprints
- D. Azure role-based access control (Azure RBAC)

Answer: B

Explanation:

<https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-w>

NEW QUESTION 127

- (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 128

- (Exam Topic 3)

Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

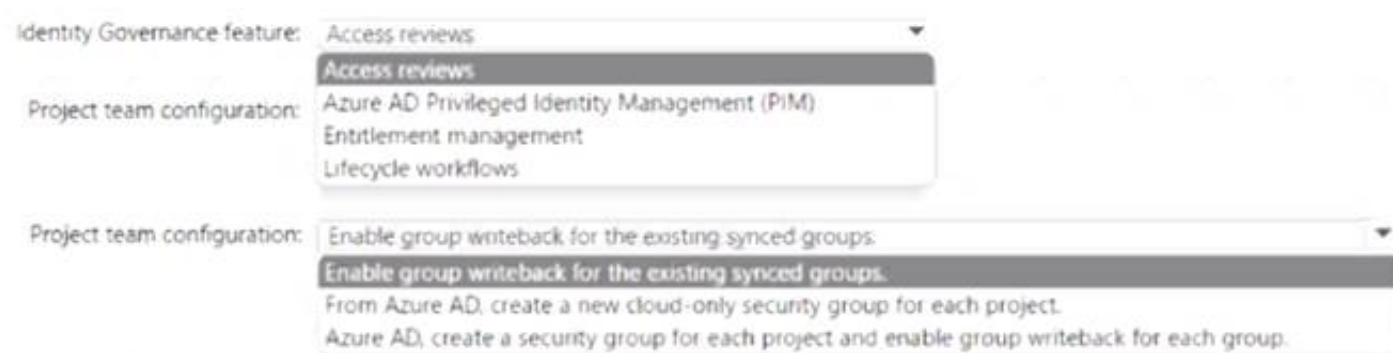
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD. Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

You need to recommend an Azure AD identity Governance solution that meets the following requirements:

- Project managers must verify that their project group contains only the current members of their project team.
- The members of each project team must only have access to the resources of the project to which they are assigned.
- Users must be removed from a project group automatically if the project manager has MOT verified the group's membership for 30 days.
- Administrative effort must be minimized.

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



NEW QUESTION 129

- (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

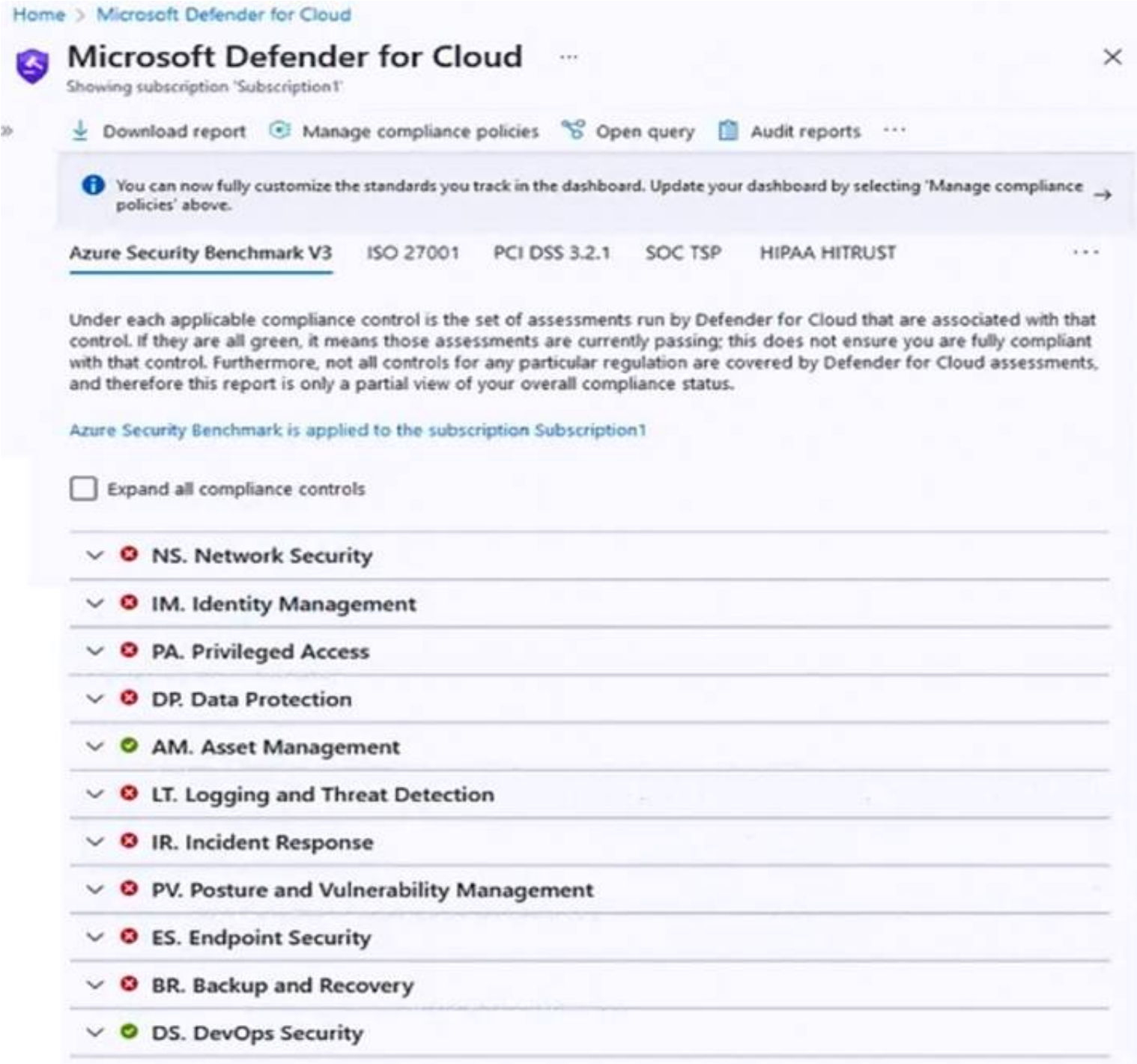
Explanation:

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

NEW QUESTION 134

- (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 137

- (Exam Topic 3)

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

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

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

Answer Area

Service:

Policy type:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Service:

Policy type:

NEW QUESTION 140

- (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 145

- (Exam Topic 3)

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

- Prevent the need to enable ports 3389 and 22 from the internet.
- Only provide permission to connect the virtual machines when required.
- Ensure that administrators use the Azure portal to connect to the virtual machines.

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

- A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
- B. Configure Azure VPN Gateway.
- C. Enable Just Enough Administration (JEA).
- D. Enable just-in-time (JIT) VM access.
- E. Configure Azure Bastion.

Answer: DE

Explanation:

<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

NEW QUESTION 148

- (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 149

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscrip 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 151

- (Exam Topic 3)

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

You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Manage NSG rules by using:

- Just-in-time (JIT) VM access
- Azure Automation
- Azure Bastion
- Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from:

- Any public IP addresses provided before the connection is established
- Any public IP addresses provided before the connection is established
- AzureBastionSubnet
- GatewaySubnet

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Manage NSG rules by using:

- Just-in-time (JIT) VM access
- Azure Automation
- Azure Bastion
- Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from:

- Any public IP addresses provided before the connection is established
- Any public IP addresses provided before the connection is established
- AzureBastionSubnet
- GatewaySubnet

NEW QUESTION 152

- (Exam Topic 3)

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

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

NOTE: Each correct answer is worth one point.

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

Answer: AD

NEW QUESTION 156

- (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 158

- (Exam Topic 3)

You have an Azure subscription.

Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.

What should you recommend using to enforce the governance requirement?

- A. regulatory compliance standards in Microsoft Defender for Cloud
- B. custom Azure roles
- C. Azure Policy assignments
- D. Azure management groups

Answer: C

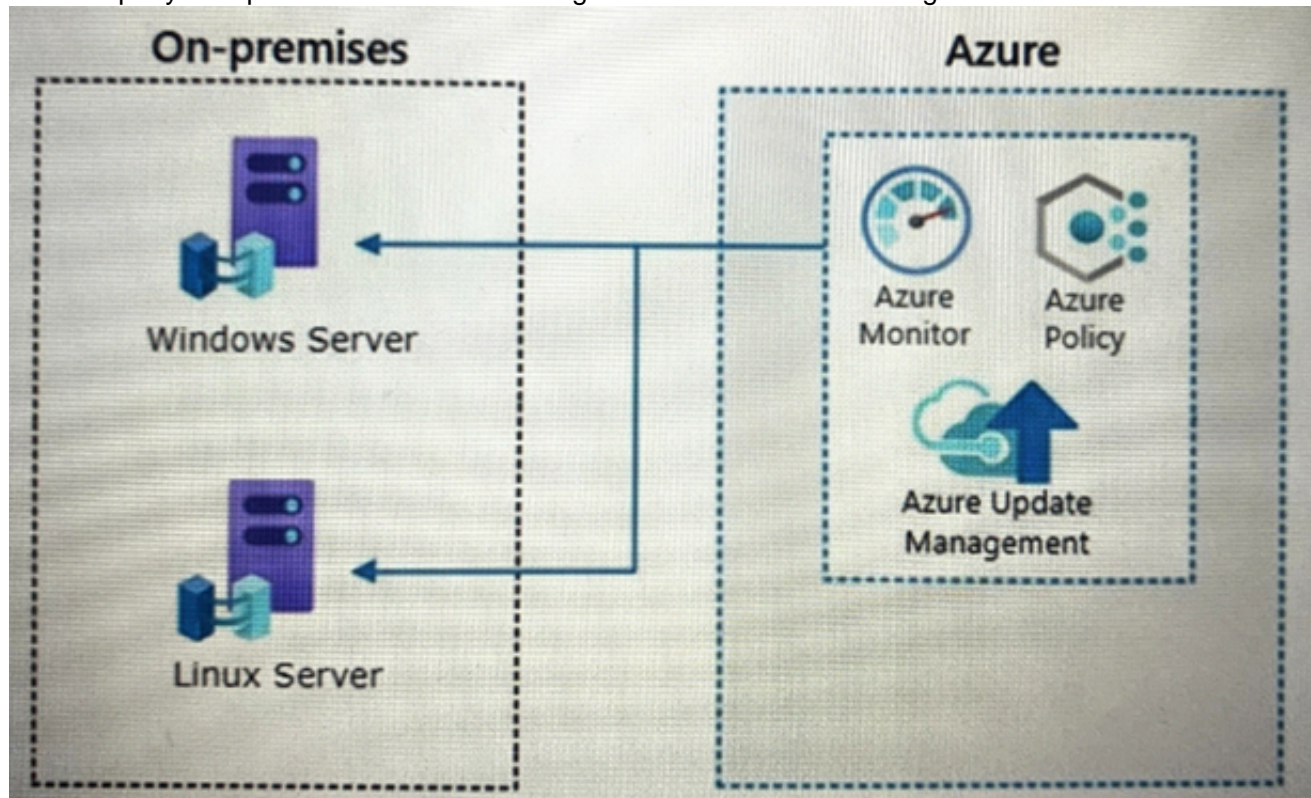
NEW QUESTION 162

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

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



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

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

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

NOTE Each correct selection is worth one point.

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

Answer: BE

Explanation:

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

NEW QUESTION 163

- (Exam Topic 3)

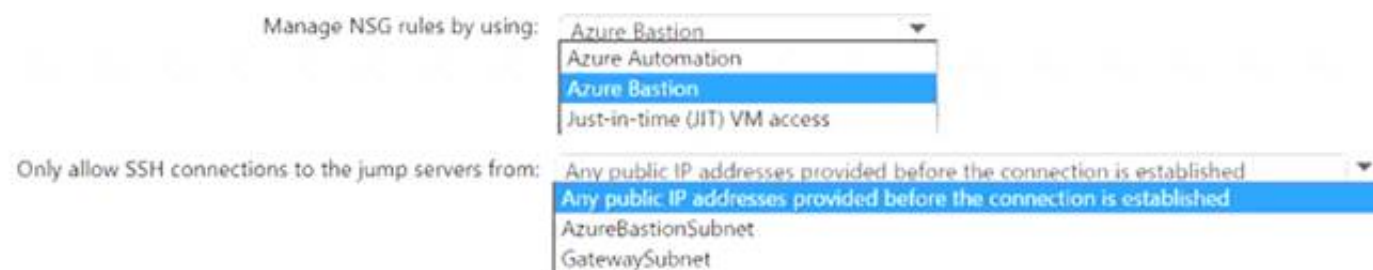
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group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

You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:

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

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

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 167

- (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 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 Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses Microsoft-managed keys.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

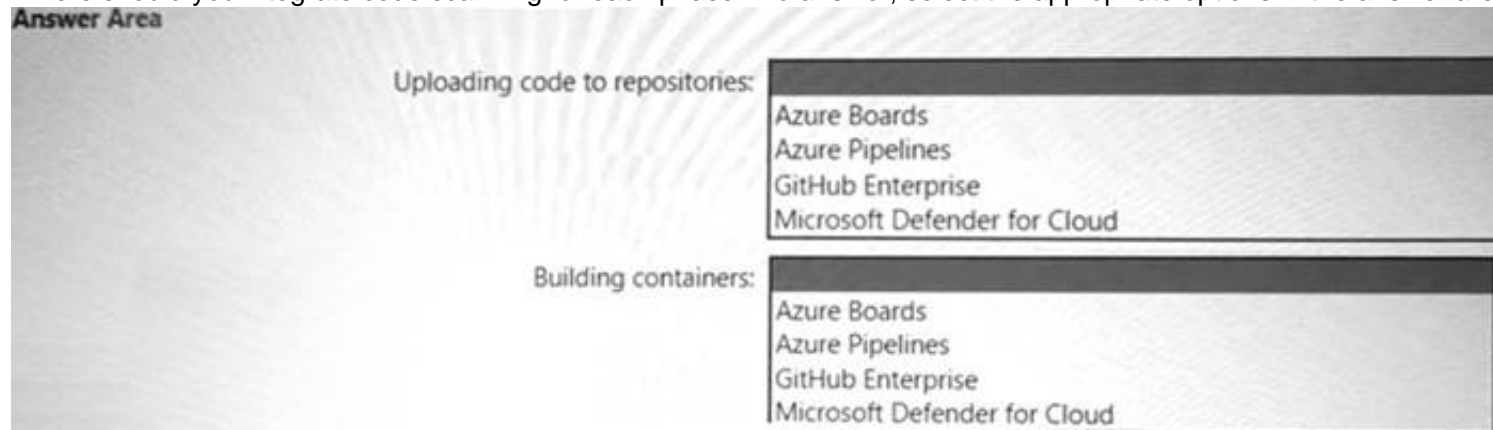
NEW QUESTION 170

- (Exam Topic 3)

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

Uploading the code to repositories Building containers

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec> <https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-conta>

NEW QUESTION 174

- (Exam Topic 3)

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities.

You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

- A. standalone sensors
- B. honeypot entity tags
- C. sensitivity labels
- D. custom user tags

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeypot-activity> The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

NEW QUESTION 177

- (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 181

- (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:

Build and test

Commit the code

Go to production

Operate

Plan and develop

Static application security testing:

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:

Build and test

Commit the code

Go to production

Operate

Plan and develop

Static application security testing:

Build and test

Commit the code

Go to production

Operate

Plan and develop

NEW QUESTION 186

- (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:

Secure deployment credentials:

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Git workflow:

Secure deployment credentials:

NEW QUESTION 191

- (Exam Topic 3)

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

- When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.
- When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.

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

Answer Area

For the database administrators:

For the operators:

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

For the database administrators:

For the operators:

NEW QUESTION 196

- (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 199

- (Exam Topic 3)

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Your on-premises network contains firewalls that support forwarding event logs in the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls.

You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include in the recommendation?

- A. an Azure logic app
- B. an on-premises Syslog server
- C. an on-premises data gateway
- D. Azure Data Factory

Answer: B

NEW QUESTION 200

- (Exam Topic 3)

You have an Azure subscription. The subscription contains 100 virtual machines that run Windows Server. The virtual machines are managed by using Azure Policy and Microsoft Defender for Servers.

You need to enhance security on the virtual machines. The solution must meet the following requirements:

- Ensure that only apps on an allowlist can be run.
- Require administrators to confirm each app added to the allowlist.
- Automatically add unauthorized apps to a blocklist when an attempt is made to launch the app.
- Require administrators to approve an app before the app can be moved from the blocklist to the allowlist. What should you include in the solution?

- A. a compute policy in Azure Policy
- B. admin consent settings for enterprise applications in Azure AD
- C. adaptive application controls in Defender for Servers
- D. app governance in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 204

- (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?

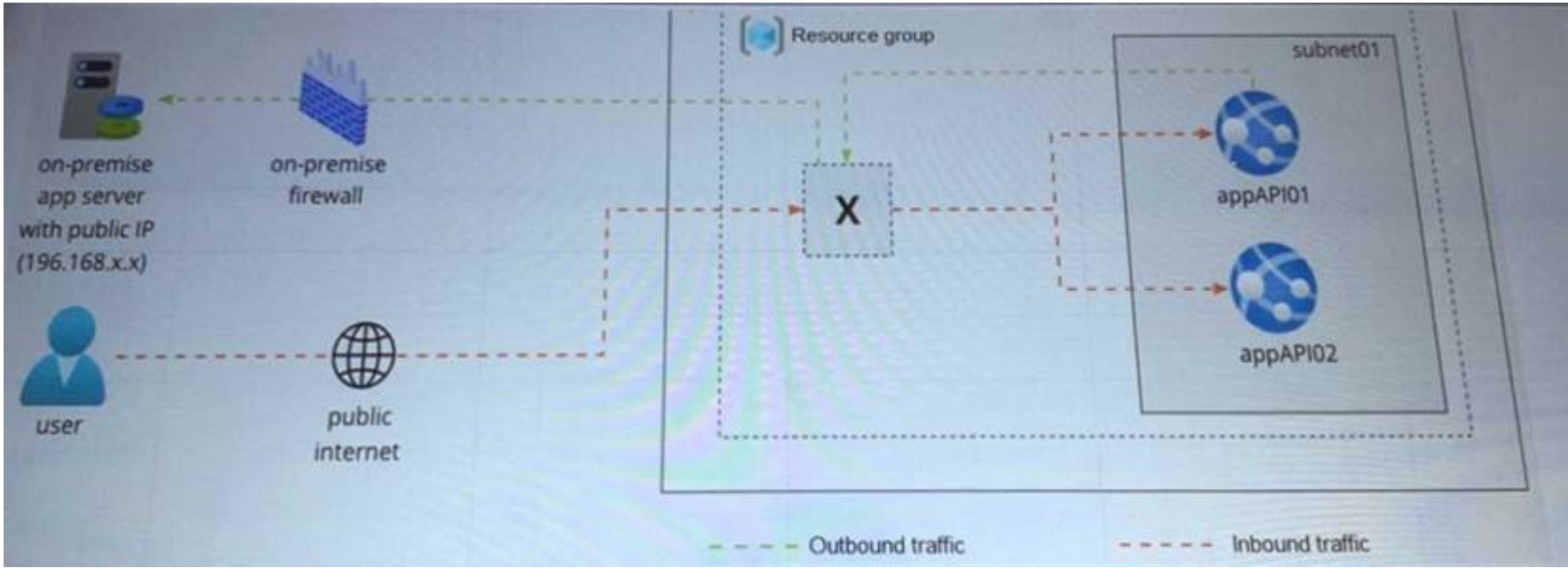
- A. Enable built-in compliance policies in Azure Policy.
- B. Enable self-healing in Microsoft 365 Defender.
- C. Automate data classification.
- D. Create hunting queries in Microsoft 365 Defender.

Answer: C

NEW QUESTION 209

- (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 212

- (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 attach 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 213

- (Exam Topic 3)
 You have a hybrid Azure AD tenant that has pass-through authentication enabled. You are designing an identity security strategy. You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities. What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features	Answer Area
Azure AD Password Protection	For brute force password attacks: <input type="text"/>
Extranet Smart Lockout (ESL)	For leaked credentials: <input type="text"/>
Password hash synchronization	

- A. Mastered
- B. Not Mastered

Answer: A

Features	Answer Area
Azure AD Password Protection	For brute force password attacks: Azure AD Password Protection
Extranet Smart Lockout (ESL)	For leaked credentials: Extranet Smart Lockout (ESL)
Password hash synchronization	

NEW QUESTION 216

- (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 based on HTTP headers that have the Front Door ID. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend>

NEW QUESTION 217

- (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 220

- (Exam Topic 3)

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

What should you include in the recommendation?

- A. Apply read-only locks on the storage accounts.
- B. Set the AllowShareKeyAccess property to false.
- C. Set the AllowBlobPublicAccess property to false.
- D. Configure automated key rotation.

Answer: A

Explanation:

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

NEW QUESTION 224

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-100 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-100 Product From:

<https://www.2passeasy.com/dumps/SC-100/>

Money Back Guarantee

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