Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1
- (Exam Topic 3)
You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.
You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

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

Answer: A

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 loT 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:	Azure Arc Microsoft Defender for Cloud Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Defender for IoT
For the AWS EC2 instances:	Azure Arc only Microsoft Defender for Cloud and Azure Arc Microsoft Defender for Cloud Apps only Microsoft Defender for Cloud only Microsoft Defender for Endpoint and Azure Arc Microsoft Defender for Endpoint only

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 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 5
- (Exam Topic 3)
You are evaluating an Azure environment for compliance.
You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.
Which effect should you use in Azure Policy?

A. Deny
B. Disabled
C. Modify
D. Append

Answer: B

Explanation:
Before looking to manage new or updated resources with your new policy definition, it's best to see how it evaluates a limited subset of existing resources, such as a test resource group. Use the enforcement mode Disabled (DoNotEnforce) on your policy assignment to prevent the effect from triggering or activity log entries from being created.
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/evaluate-impact

NEW QUESTION 6
- (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 7
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation.
You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) Conditional Access
C. Microsoft Defender for servers
D. Azure Policy
E. Microsoft Defender for Containers

Answer: BDE

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-conta

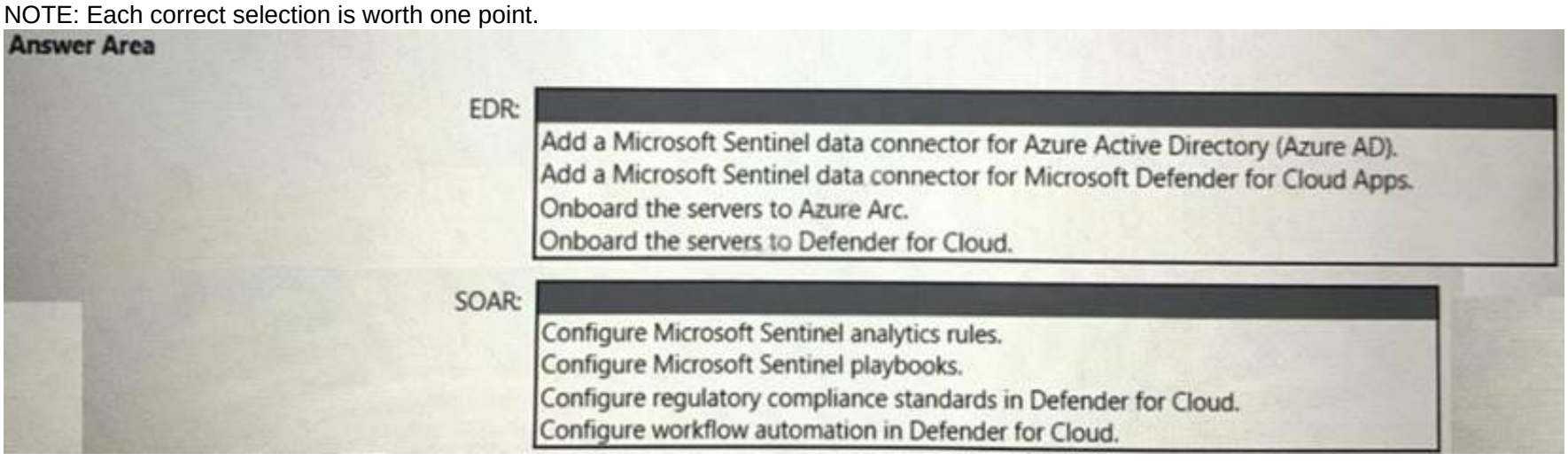
NEW QUESTION 8
- (Exam Topic 3)
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. AJI the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.
You need 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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 9
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are
configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure. You plan to deploy Azure virtual machines that will run Windows Server.
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.
How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

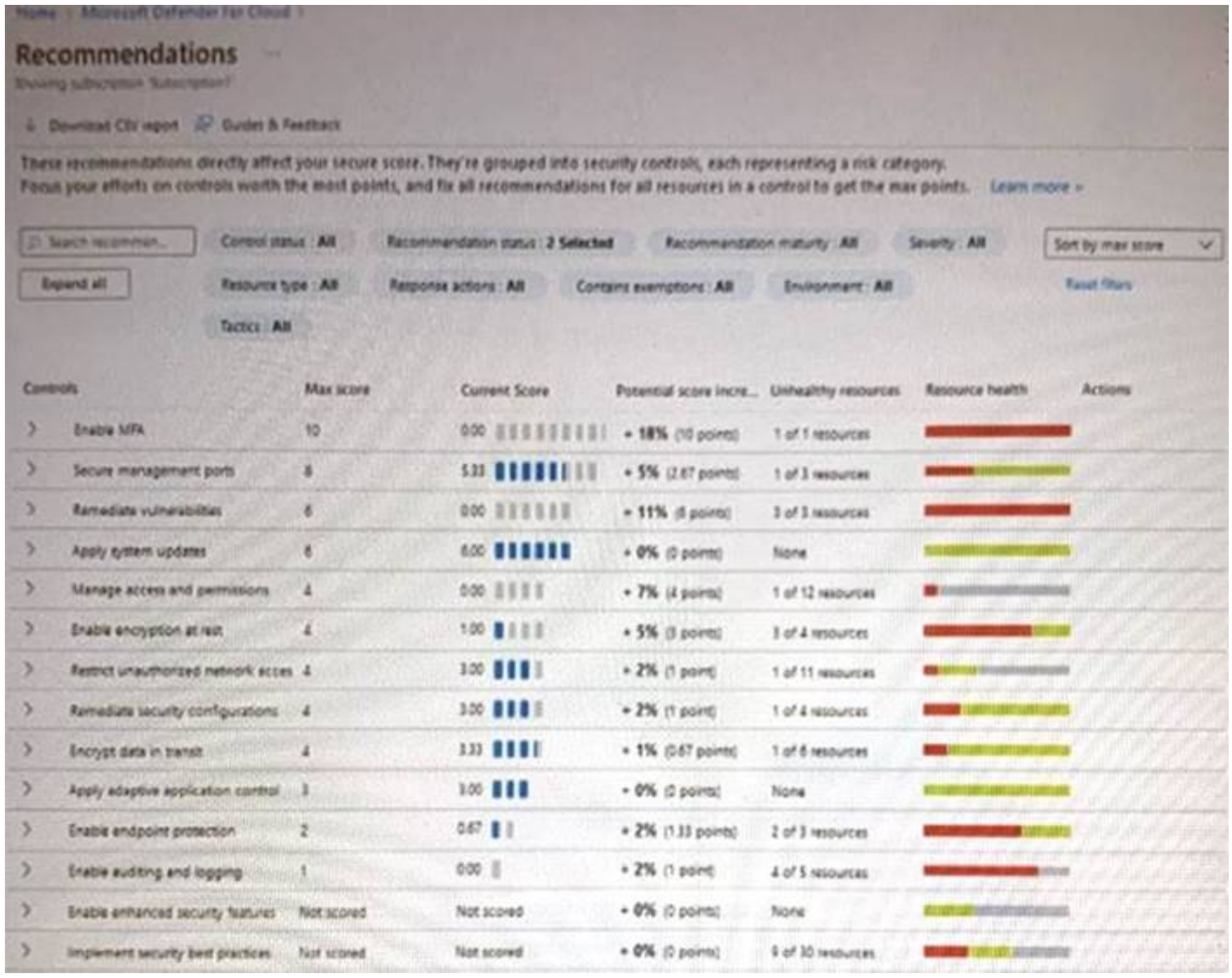


A. Mastered
B. Not Mastered

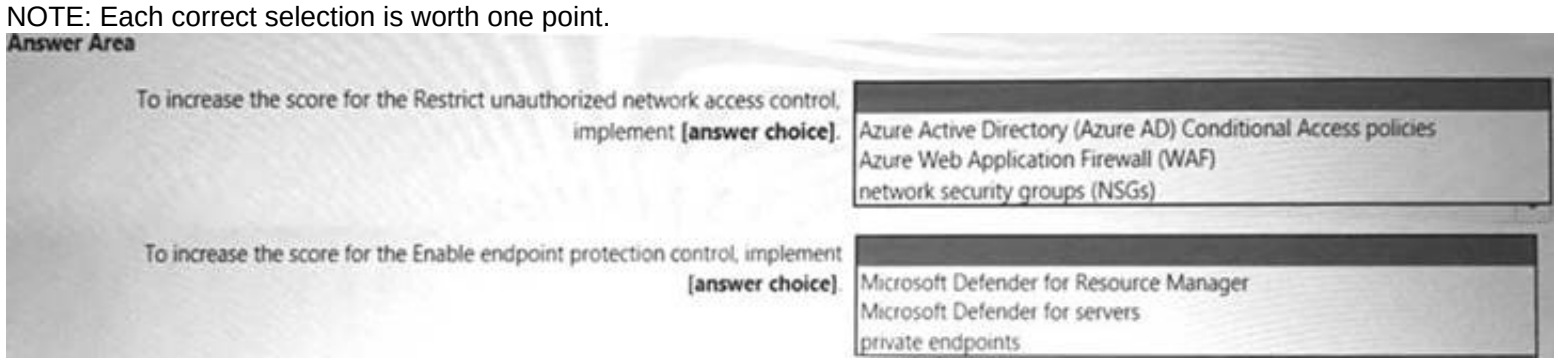
Answer: A

Explanation:
For SOAR read this https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of
Microsoft Defender.
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

NEW QUESTION 10
- (Exam Topic 3)
You open Microsoft Defender for Cloud as shown in the following exhibit.



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

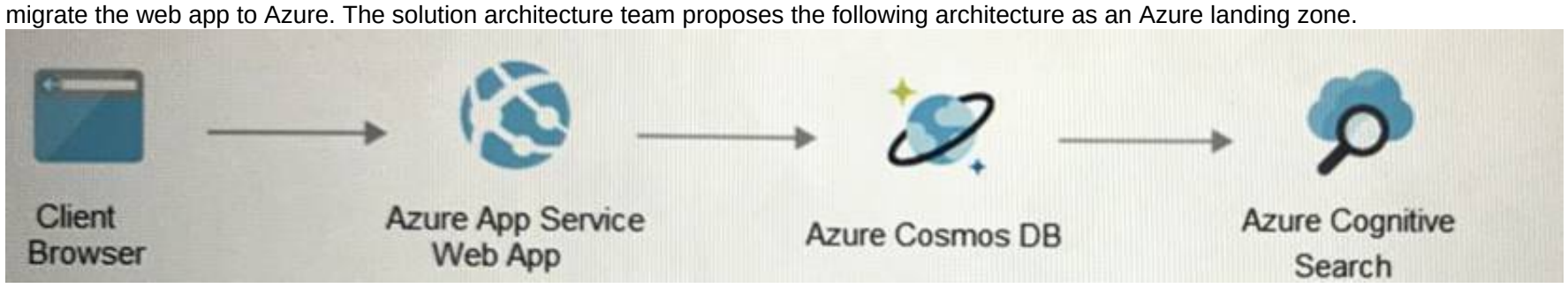


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Selection 1: NSG Selection
Selection 2: Microsoft Defender for servers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION 10
- (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 15
- (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 20
- (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 21
- (Exam Topic 3)
Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

A. Azure Firewall
B. Azure Web Application Firewall (WAF)
C. Microsoft Defender for Cloud alerts
D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)
E. Microsoft Sentinel

Answer: AB

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

NEW QUESTION 23
- (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?

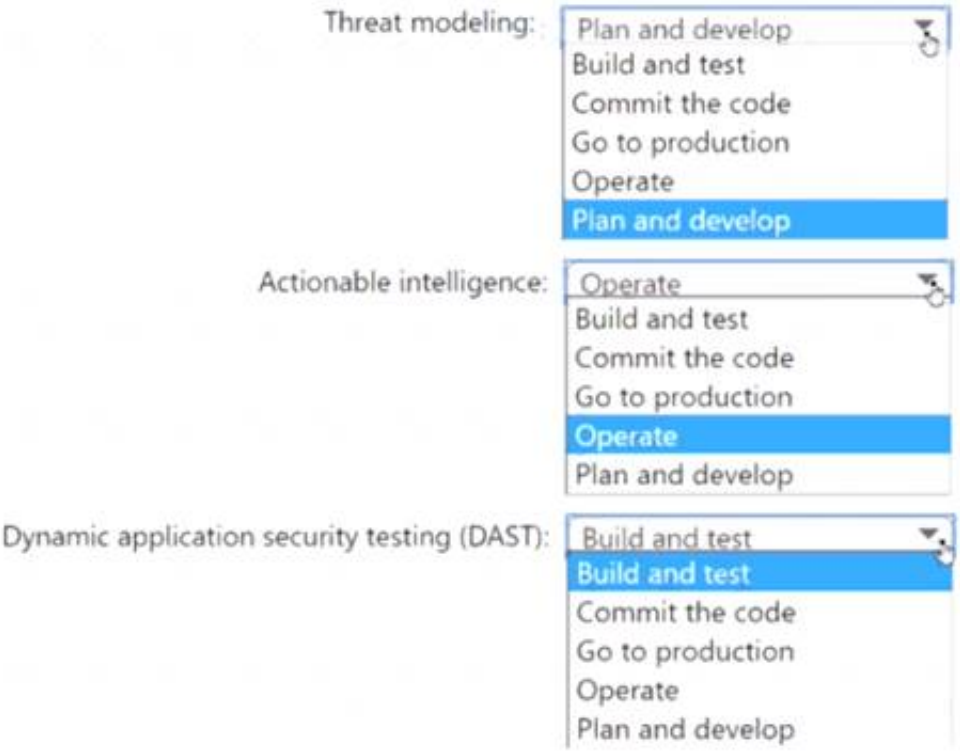
A. Enhanced Security Admin Environment (ESAE)
B. Microsoft Security Development Lifecycle (SDL)
C. Rapid Modernization Plan (RaMP)
D. Microsoft Operational Security Assurance (OSA)

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 26
- (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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

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 33
- (Exam Topic 3)
Your company has on-premises Microsoft SQL Server databases. The company plans to move the databases to Azure.
You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.
What should you include in the recommendation?

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

Answer: C

NEW QUESTION 34
- (Exam Topic 3)
You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Answer: A

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 44
- (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 (Pll) 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 likeMicrosoft 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 47
- (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.

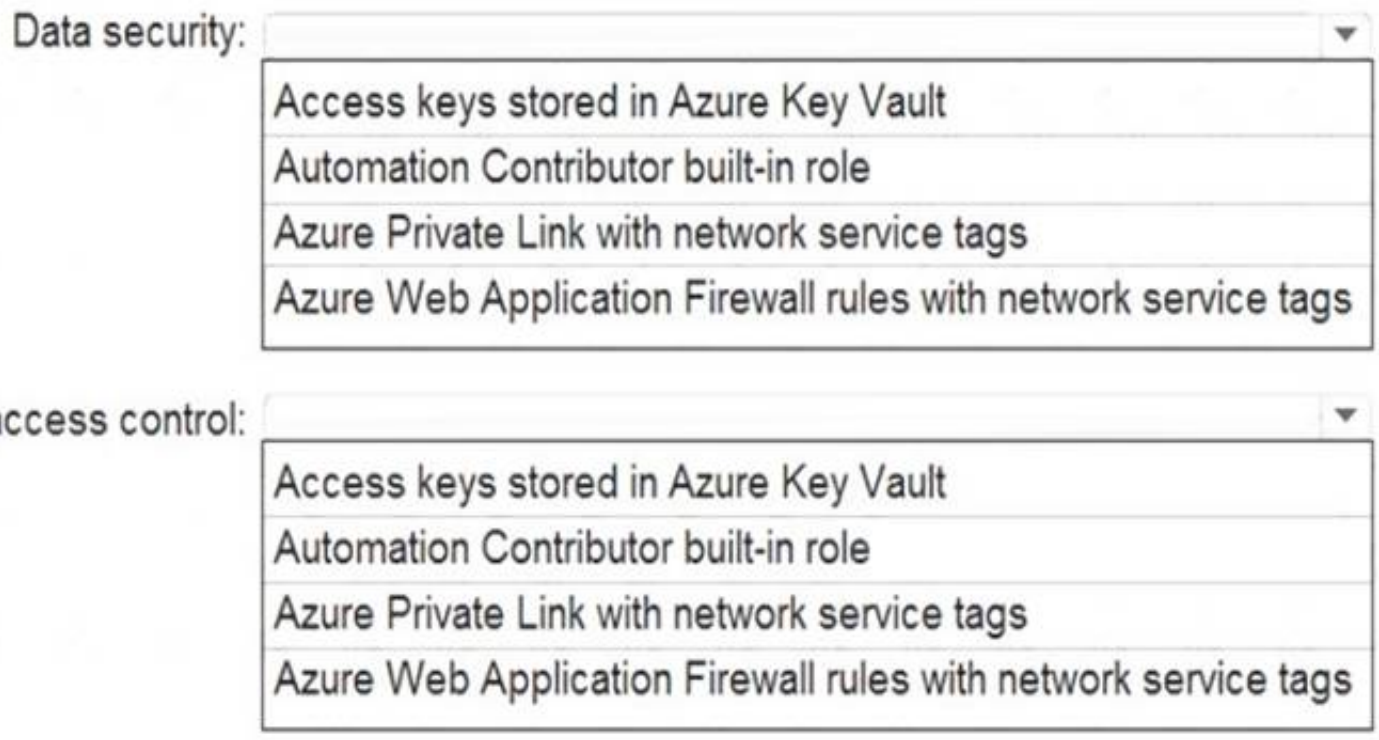
Which identity service should you include in the recommendation?

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 49
- (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.

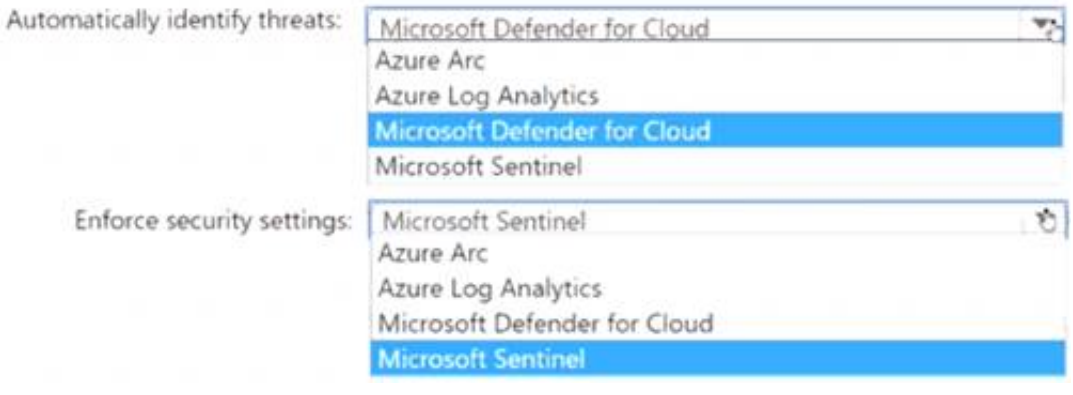


A. Mastered
B. Not Mastered

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 54
- (Exam Topic 3)
You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.
You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:
• Automatically identify threats found in AWS CloudTrail events.
• Enforce security settings on AWS virtual machines by using Azure policies.
What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area

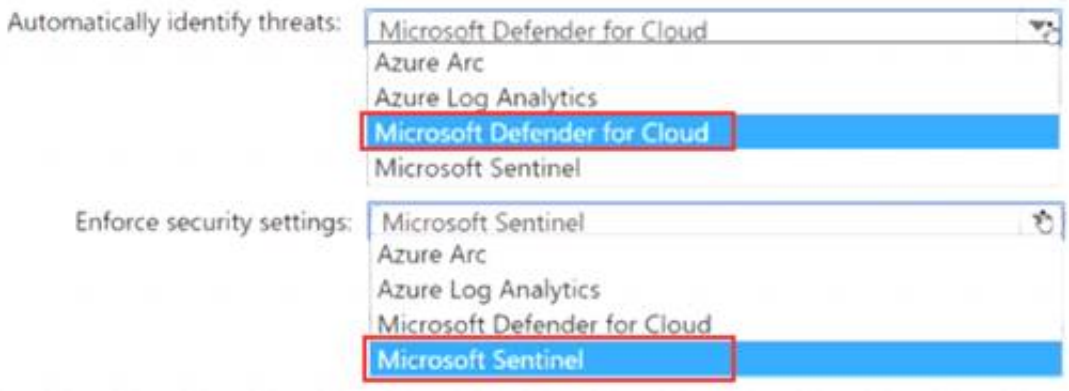


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 55
- (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 60
- (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

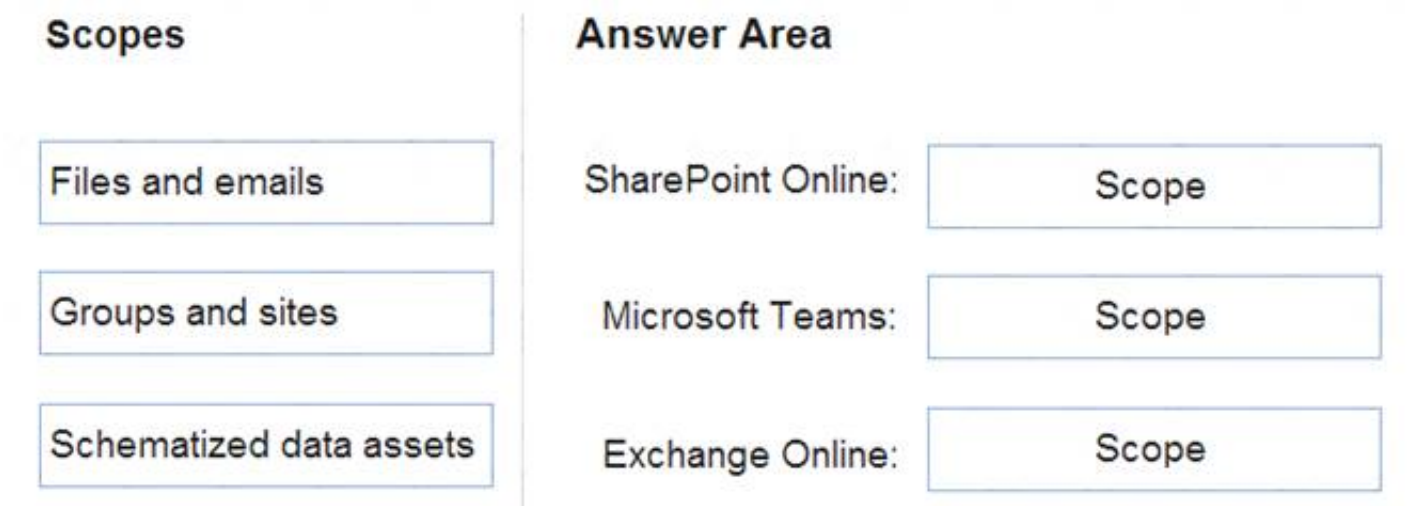
NEW QUESTION 61
- (Exam Topic 3)
Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

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

Answer: B

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

NEW QUESTION 62
- (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.



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

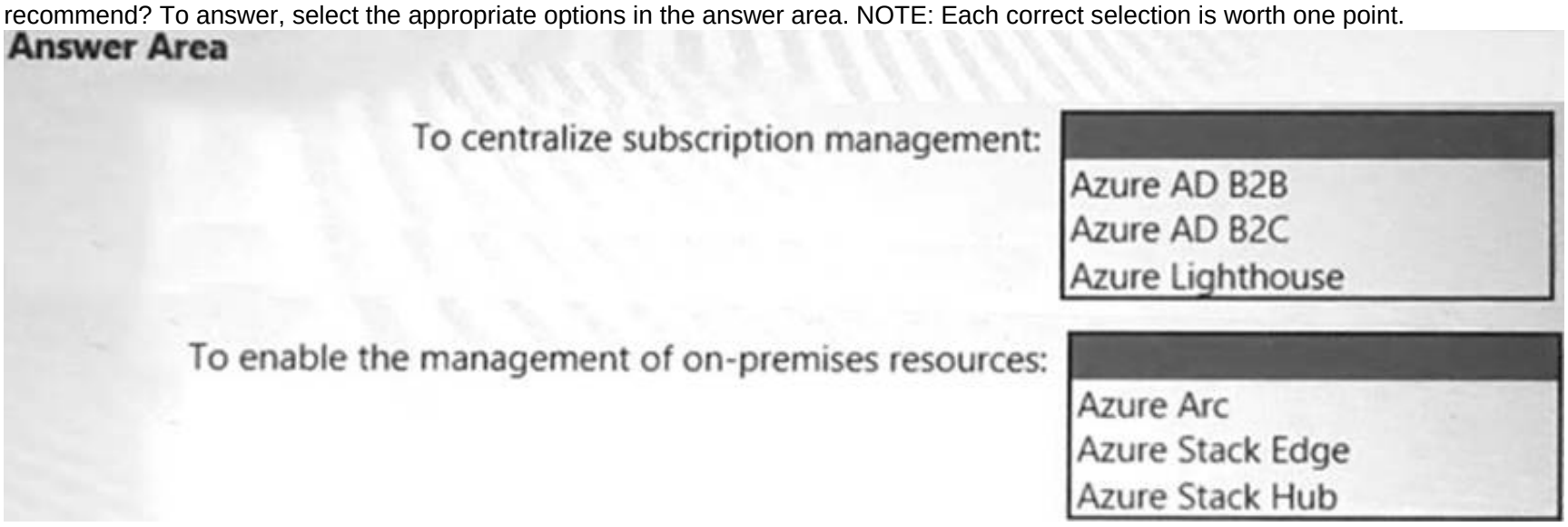
NEW QUESTION 65
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should 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

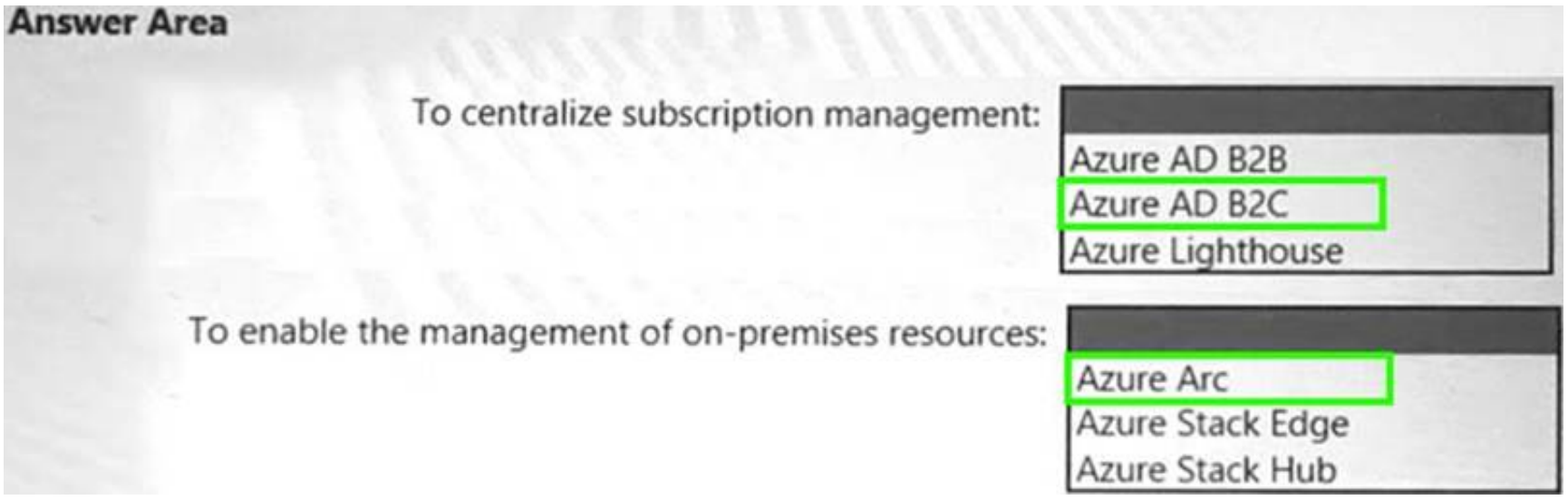
NEW QUESTION 68
- (Exam Topic 2)
You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 73
- (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

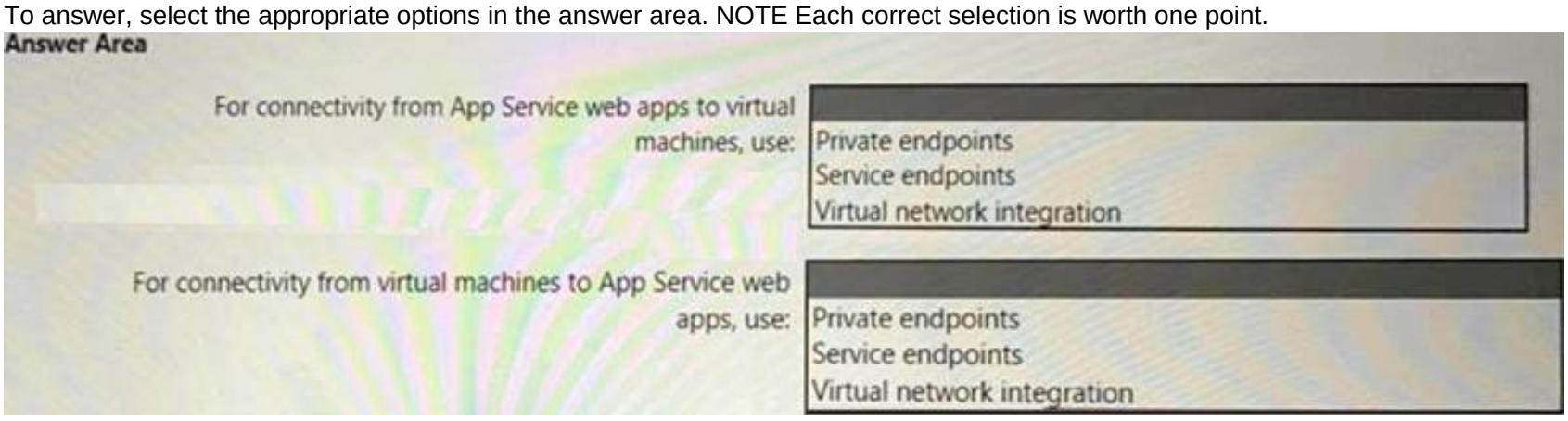
NEW QUESTION 74
- (Exam Topic 2)
You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

A. Azure AD Conditional Access
B. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. Microsoft Defender for Endpoint
E. access reviews in Azure AD

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#c https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cl

NEW QUESTION 75
- (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.



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 76
- (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 78
- (Exam Topic 1)
You need to recommend a solution to meet the compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To enforce compliance to the regulatory standard, create:	An Azure Automation account A blueprint A managed identity Workflow automation
To exclude TestRG from the compliance assessment:	Edit an Azure blueprint Modify a Defender for Cloud workflow automation Modify an Azure policy definition Update an Azure policy assignment

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 82
- (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 87
- (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 88
- (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 91
- (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

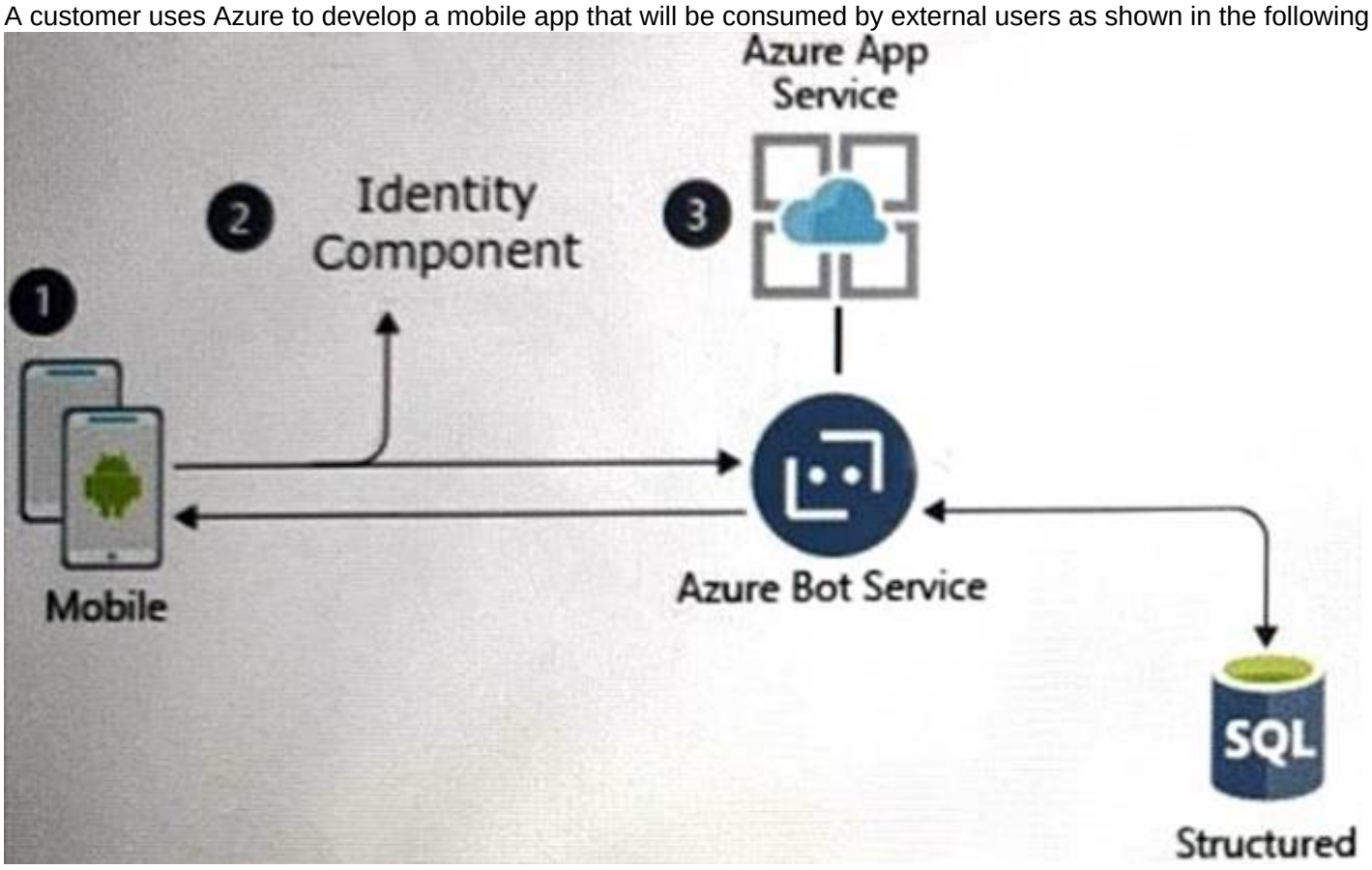
NEW QUESTION 95
- (Exam Topic 3)
Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool. Which type of diagram should you create?

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 100
- (Exam Topic 3)
A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:
• Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
• Be managed separately from the identity store of the customer.
• Support fully customizable branding for each app.

Which service should you recommend to complete the design?

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

Answer: A

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

NEW QUESTION 104
- (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 109
- (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 112
- (Exam Topic 3)
Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:
• Minimizes manual intervention by security operation analysts
• Supports Waging alerts within Microsoft Teams channels What should you include in the strategy?

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

Answer: B

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

NEW QUESTION 114
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

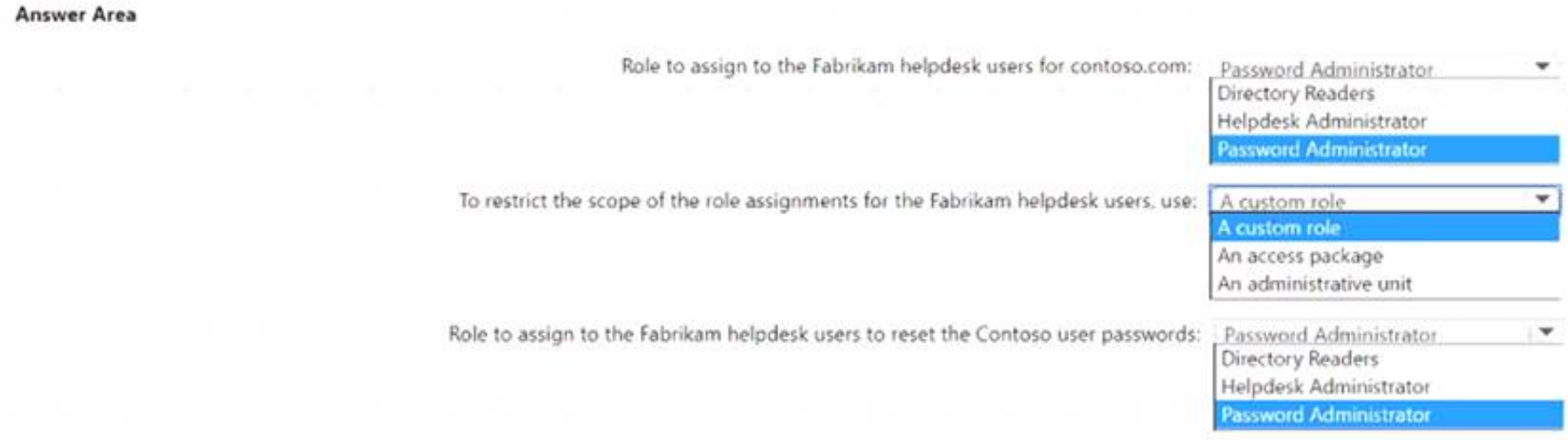
A. Yes
B. No

Answer: B

Explanation:

https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

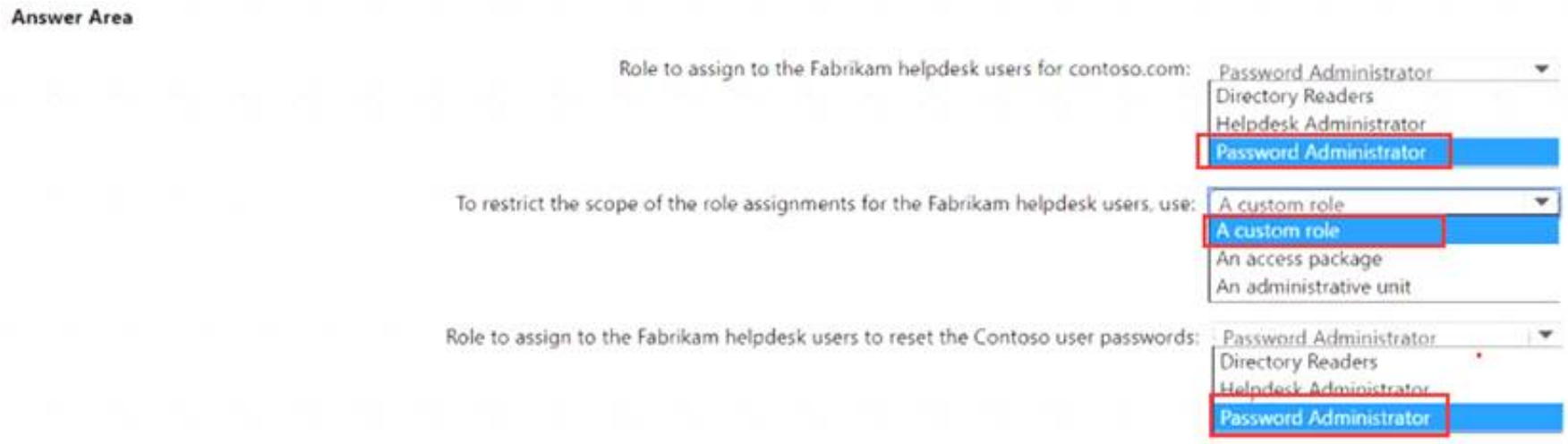
NEW QUESTION 116
- (Exam Topic 3)
Your company, named Contoso. Ltd... has an Azure AD tenant namedcontoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:
• Follow the principle of least privilege.
• Minimize administrative effort.
What should you do? 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 118
- (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

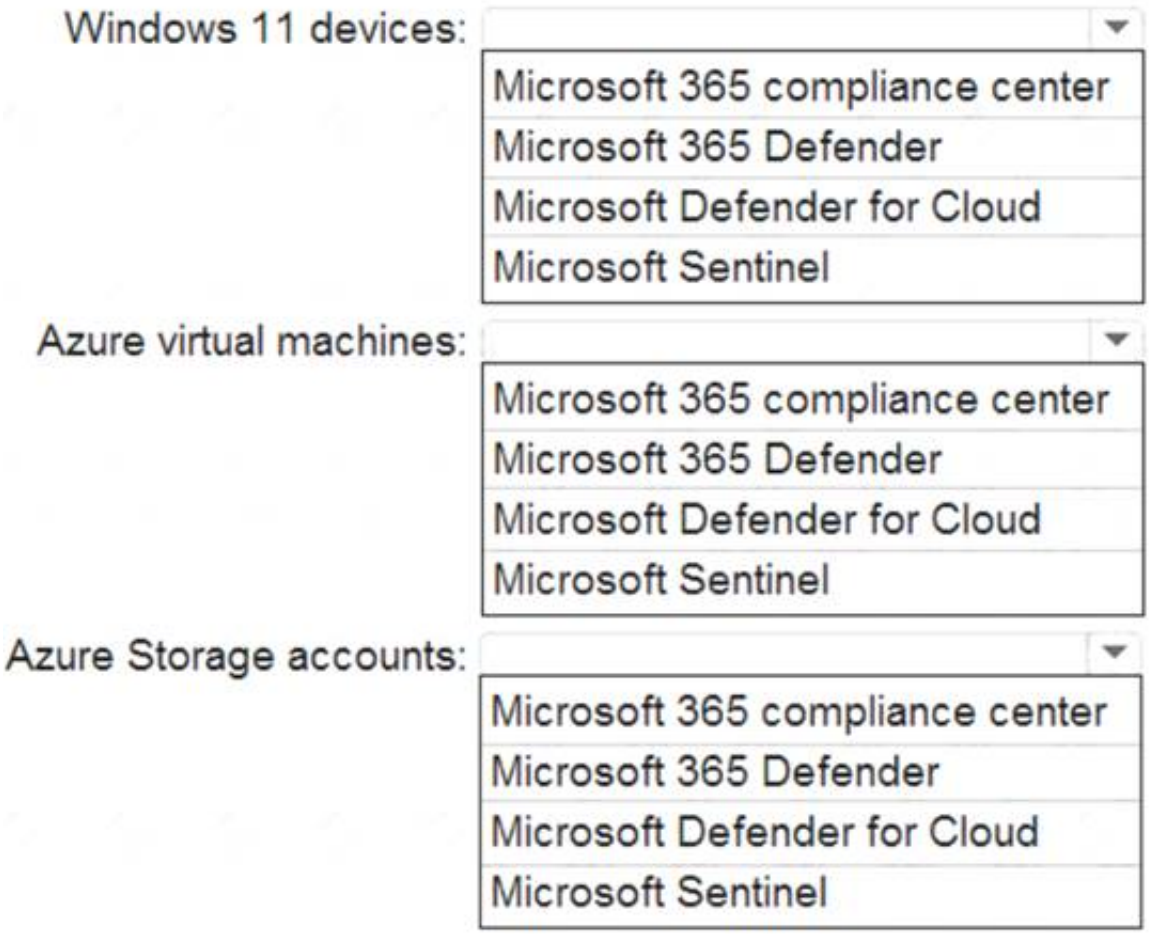
NEW QUESTION 119
- (Exam Topic 3)
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.
You need to recommend a solution for the customer. 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 120
- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscripts 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.



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

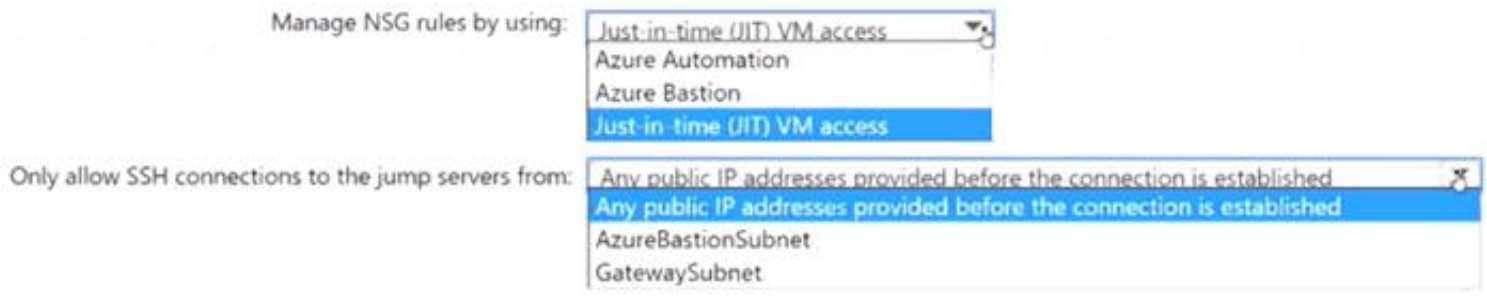
NEW QUESTION 121
- (Exam Topic 3)
Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.
You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft 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 124
- (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.

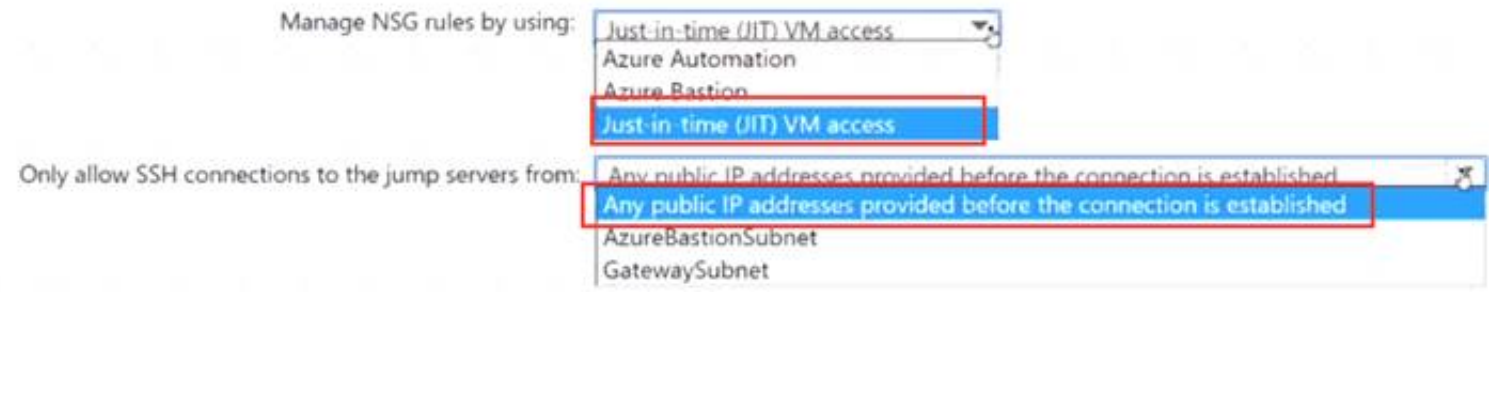
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 129
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.
The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
• Prevent the remote users from accessing any other resources on the network.
• Support Azure Active Directory (Azure AD) Conditional Access.
• Simplify the end-user experience.
What should you include in the recommendation?

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

Answer: A

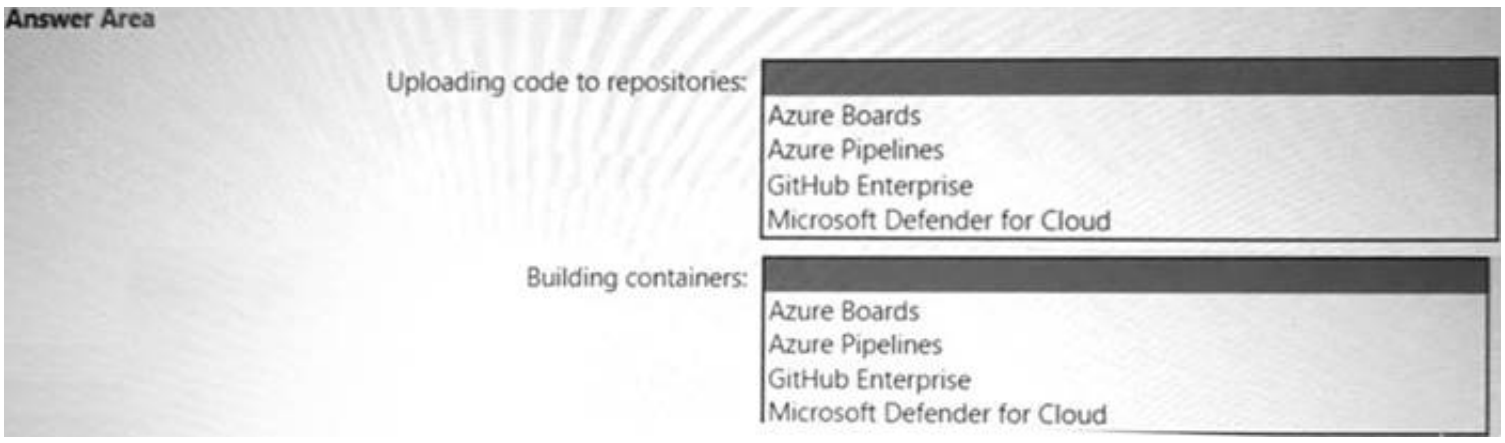
Explanation:
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

NEW QUESTION 134
- (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 136
- (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 140
- (Exam Topic 3)
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.
Which three actions should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Implement Azure Firewall to restrict host pool outbound access.
C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
E. Deploy a Remote Desktop server to an Azure region located in France.

Answer: BCD

Explanation:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

NEW QUESTION 143
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance. What should you do first?

A. From Defender for Cloud, review the secure score recommendations.
B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.
C. From Defender for Cloud, review the Azure security baseline for audit report.
D. From Defender for Cloud, add a regulatory compliance standard.

Answer: D

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

NEW QUESTION 144
- (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:

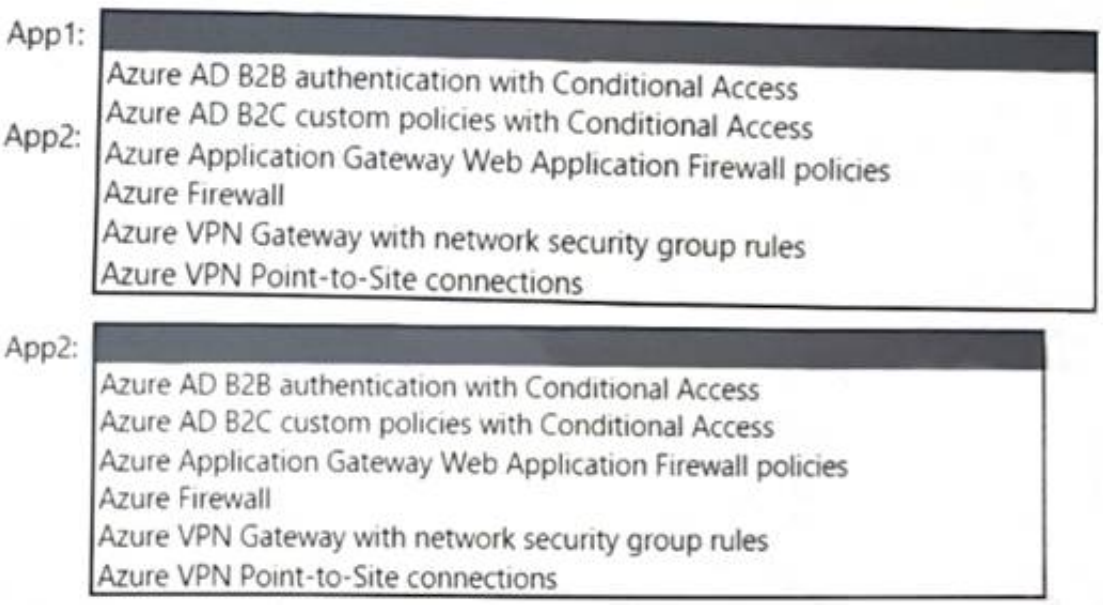
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-acc

NEW QUESTION 147
- (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



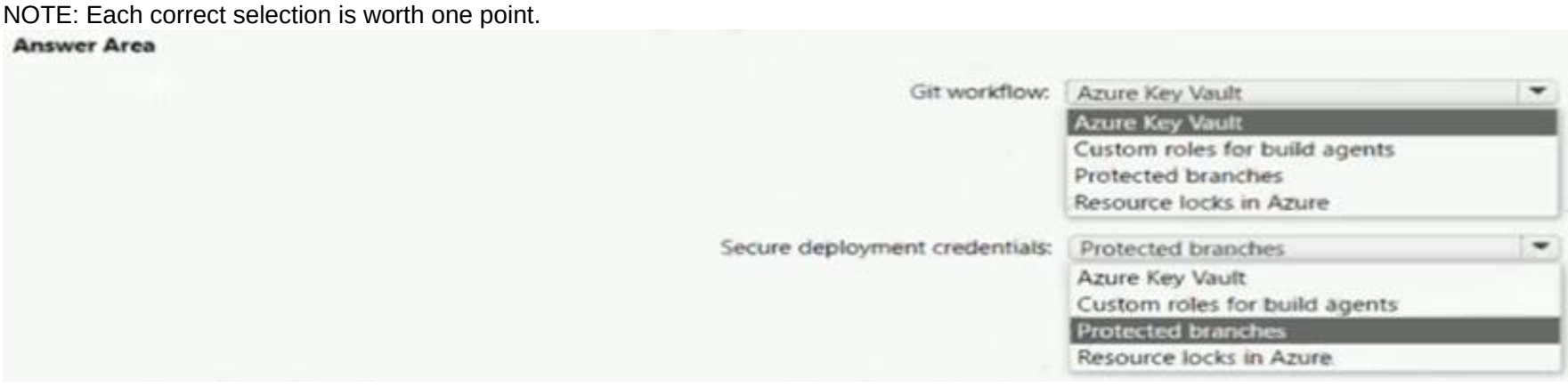
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence

NEW QUESTION 149
- (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

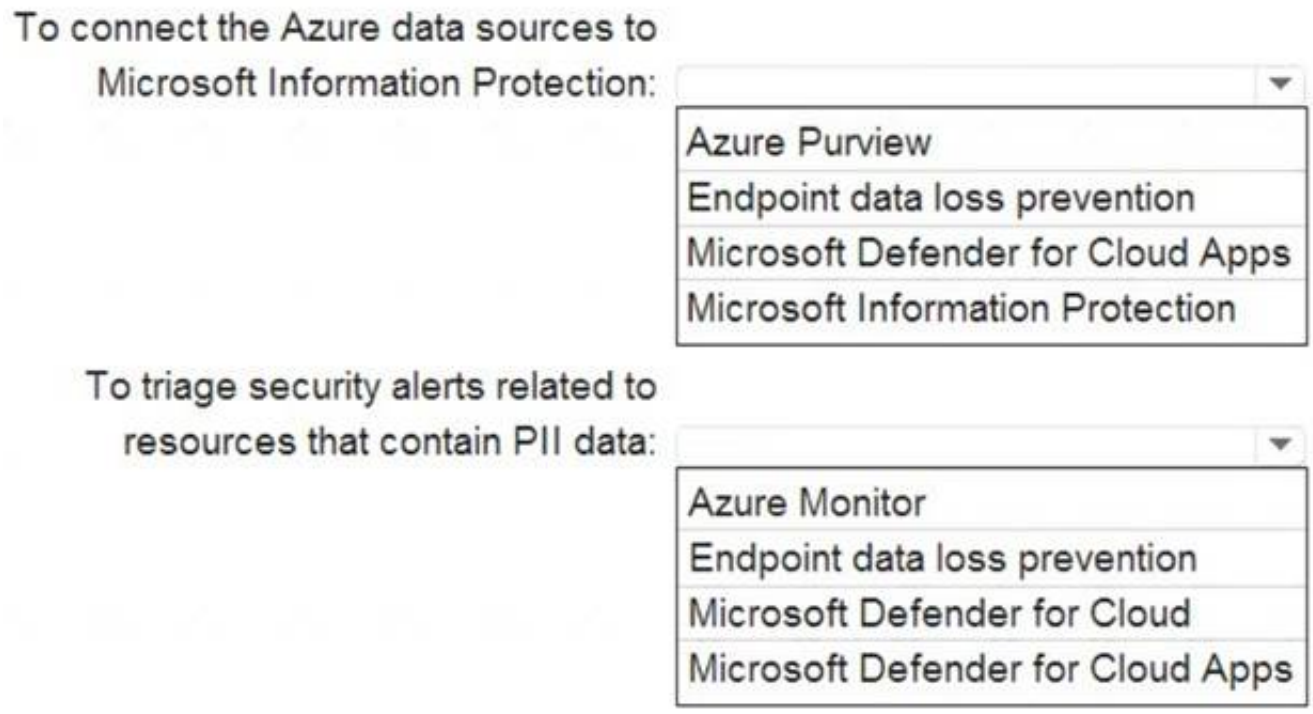


A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 153
- (Exam Topic 3)
Your company is migrating data to Azure. The data contains Personally Identifiable Information (Pll). The
company plans to use Microsoft Information Protection for the Pll data store in Azure. You need to recommend a solution to discover Pll data at risk in the Azure resources.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

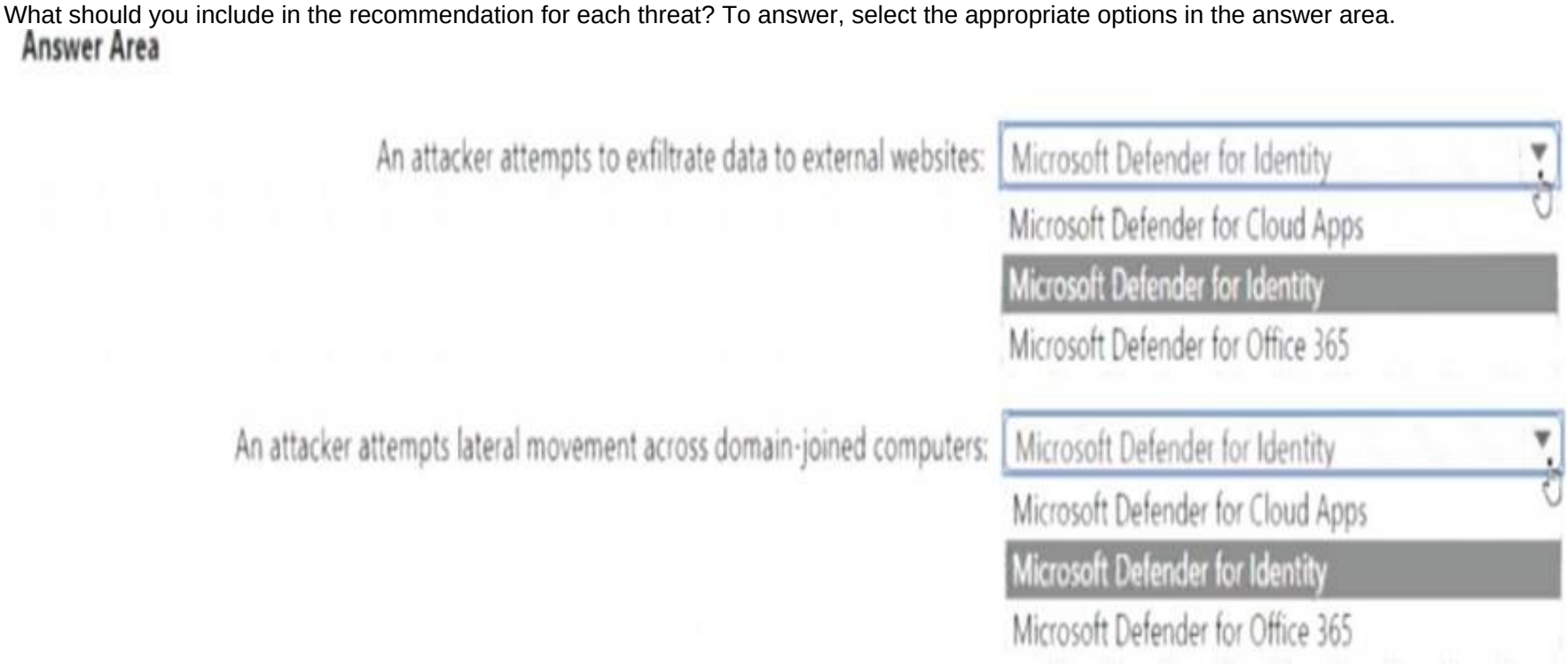


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Prioritize security actions by data sensitivity,
https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection. As to Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure resources as well): https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azu

NEW QUESTION 157
- (Exam Topic 3)
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA). You need to protect against the following external threats of an attack chain:
• An attacker attempts to exfiltrate data to external websites.
• An attacker attempts lateral movement across domain-joined computers.
What should you include in the recommendation for each threat? To answer, select the appropriate options in the answer area.

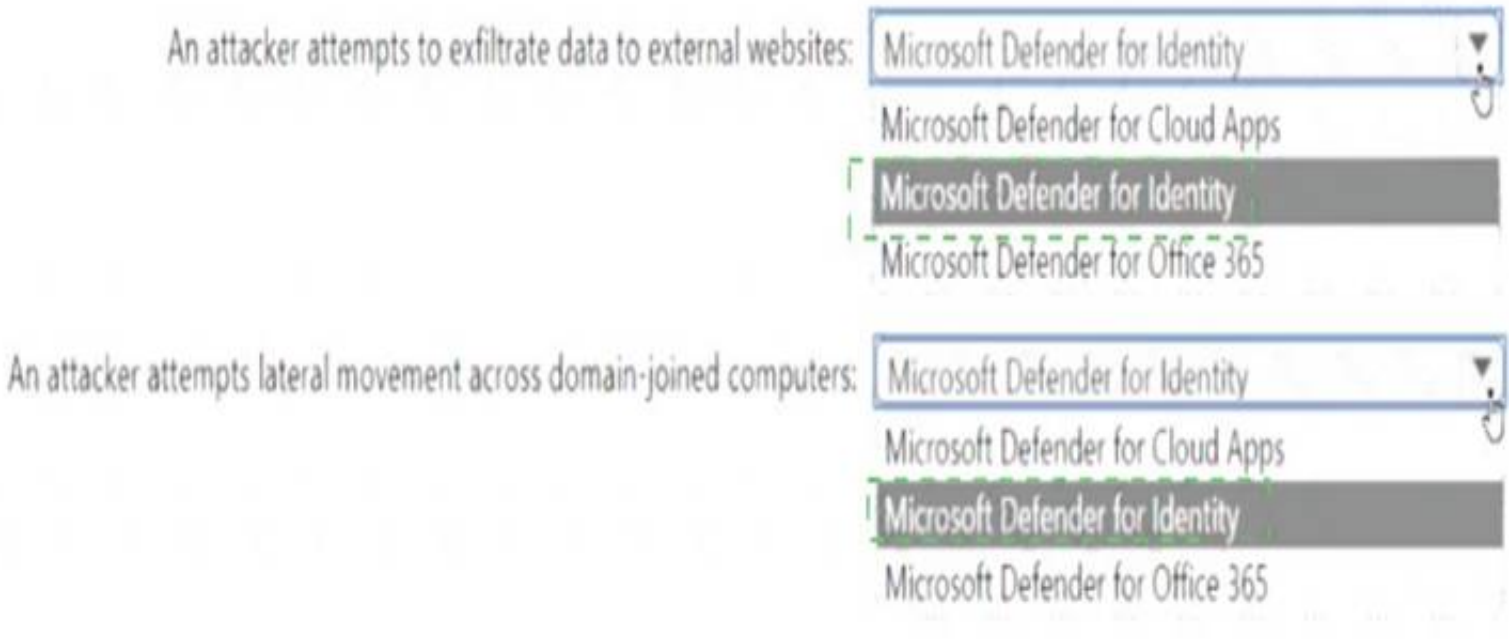


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

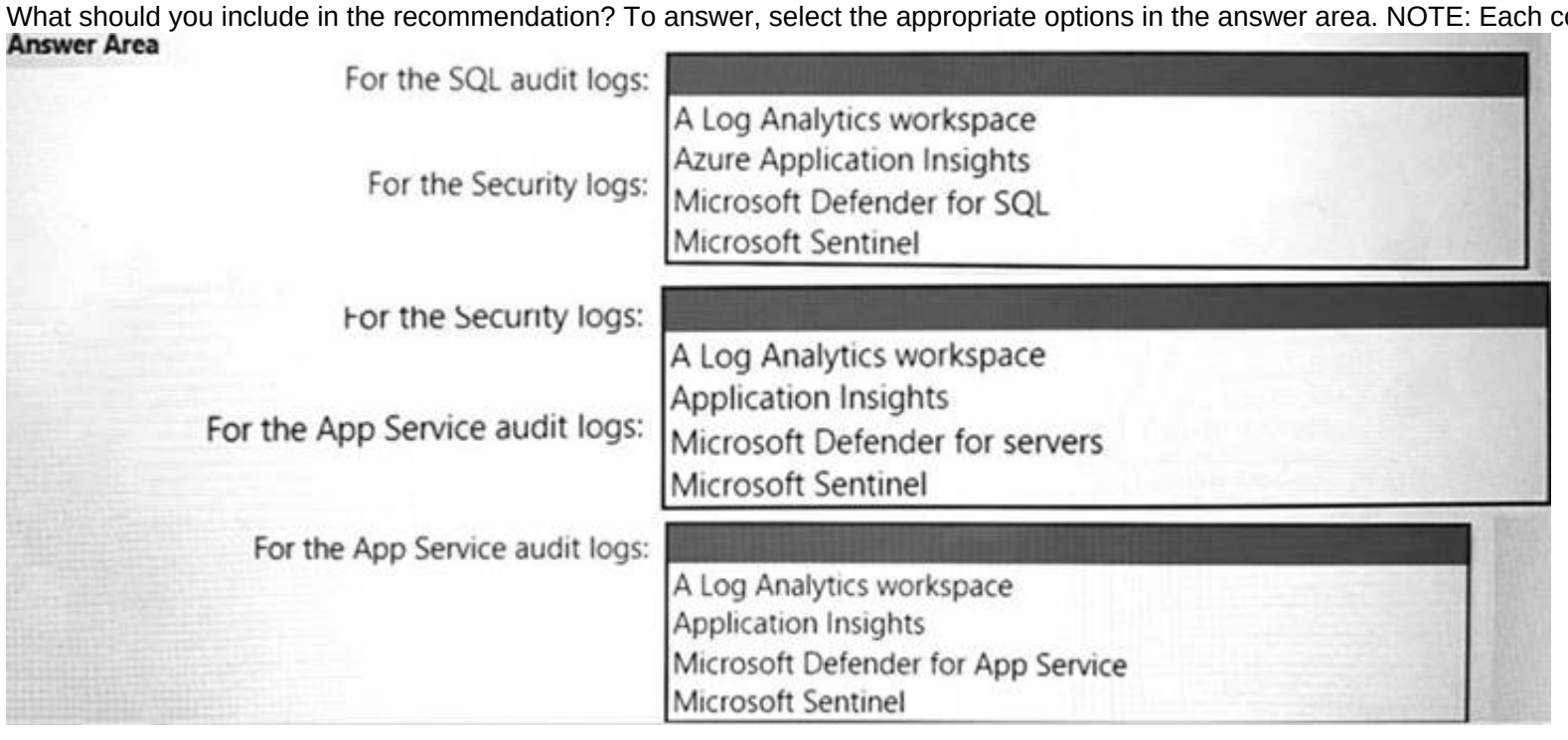


NEW QUESTION 162
- (Exam Topic 3)
You have an Azure subscription that contains a Microsoft Sentinel workspace.
Your on-premises network contains firewalls that support forwarding event logs m the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls
You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include m 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 166
- (Exam Topic 3)
You are designing an auditing solution for Azure landing zones that will contain the following components:
• SQL audit logs for Azure SQL databases
• Windows Security logs from Azure virtual machines
• Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
• Log all privileged access.
• Retain logs for at least 365 days.
• Minimize costs.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

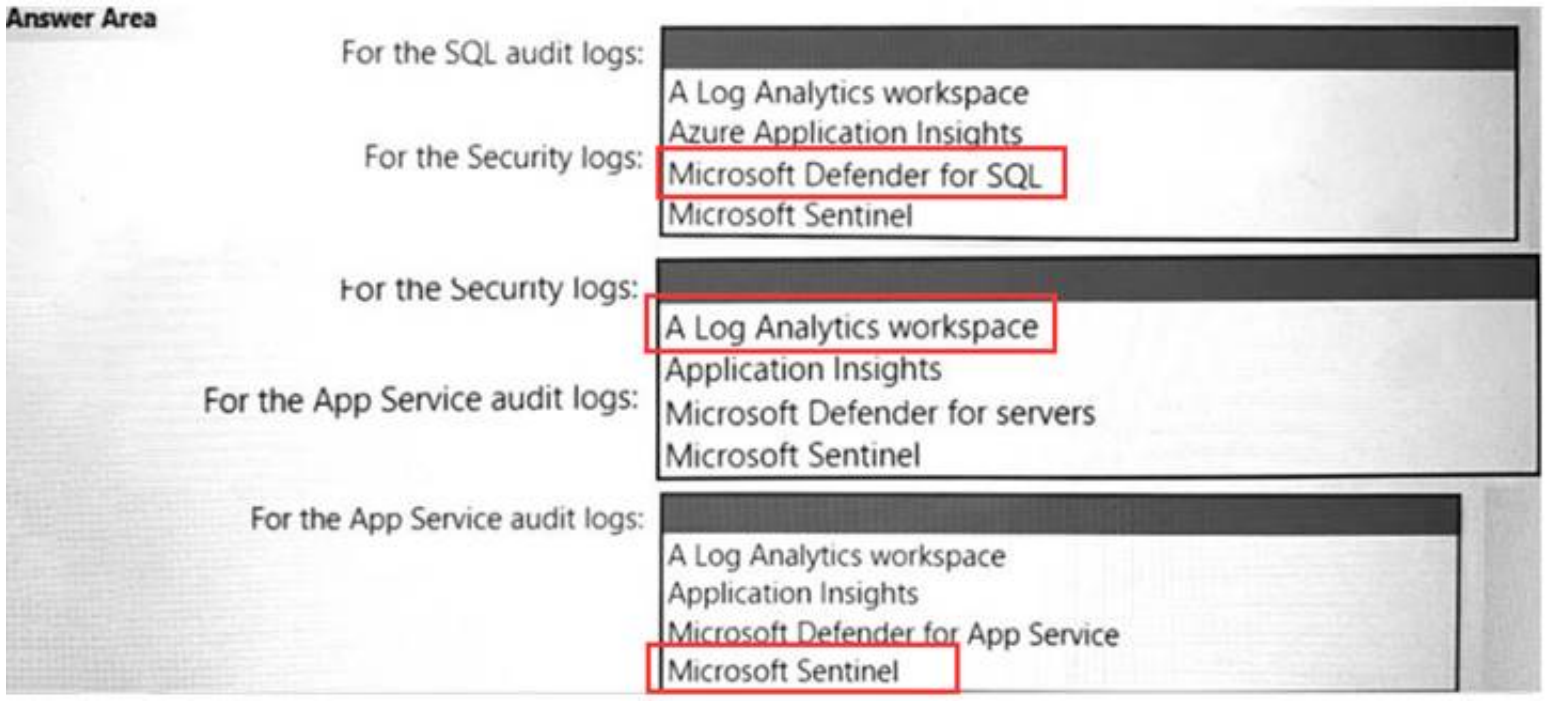


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 168
- (Exam Topic 3)
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.

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

Answer: AF

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

NEW QUESTION 172
- (Exam Topic 3)
You have the following on-premises servers that run Windows Server:
• Two domain controllers in an Active Directory Domain Services (AD DS) domain
• Two application servers named Server1 and Server2 that run ASP.NET web apps
• A VPN server named Server3 that authenticates by using RADIUS and AD DS End users use a VPN to access the web apps over the internet.
You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).
What should you include in the recommendation?

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

Answer: C

NEW QUESTION 174
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 176
- (Exam Topic 3)
You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.
All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful

ransomware attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Use Azure Monitor notifications when backup configurations change.
B. Require PINs for critical operations.
C. Perform offline backups to Azure Data Box.
D. Encrypt backups by using customer-managed keys (CMKs).
E. Enable soft delete for backups.

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware 'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.' Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

NEW QUESTION 181
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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