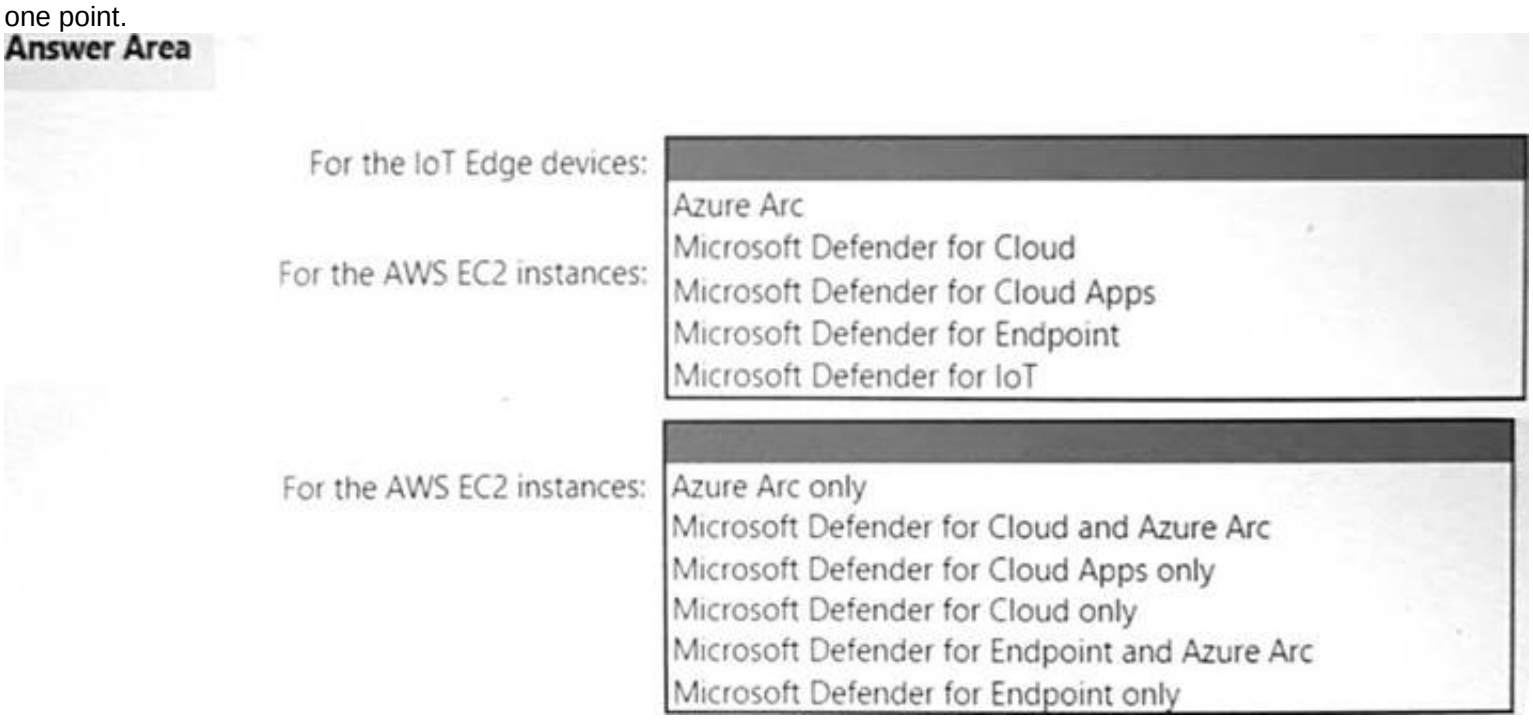
Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1
- (Exam Topic 3)
Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:
• Azure IoT Edge devices
• AWS EC2 instances
Which services should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

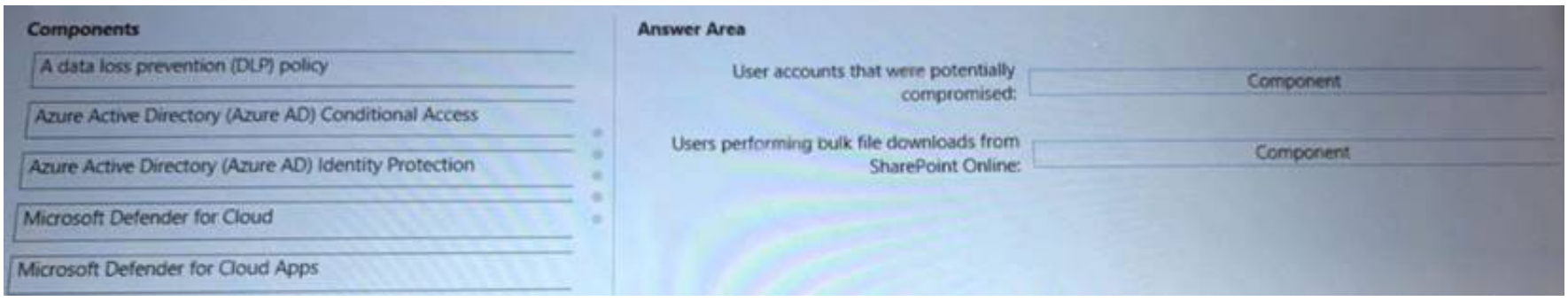


A. Mastered
B. Not Mastered

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 2
- (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 3
- (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

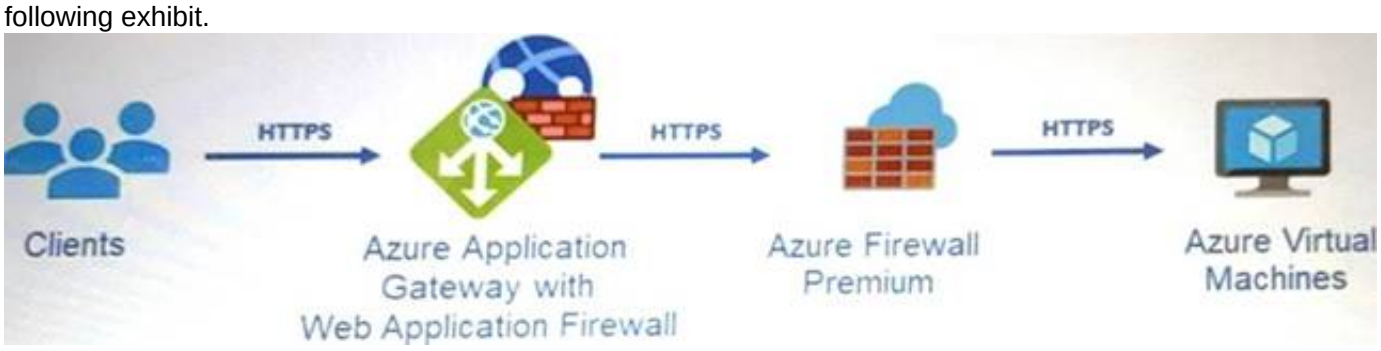
The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure. You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks
such as ransomware.
What should you include in the recommendation?

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.

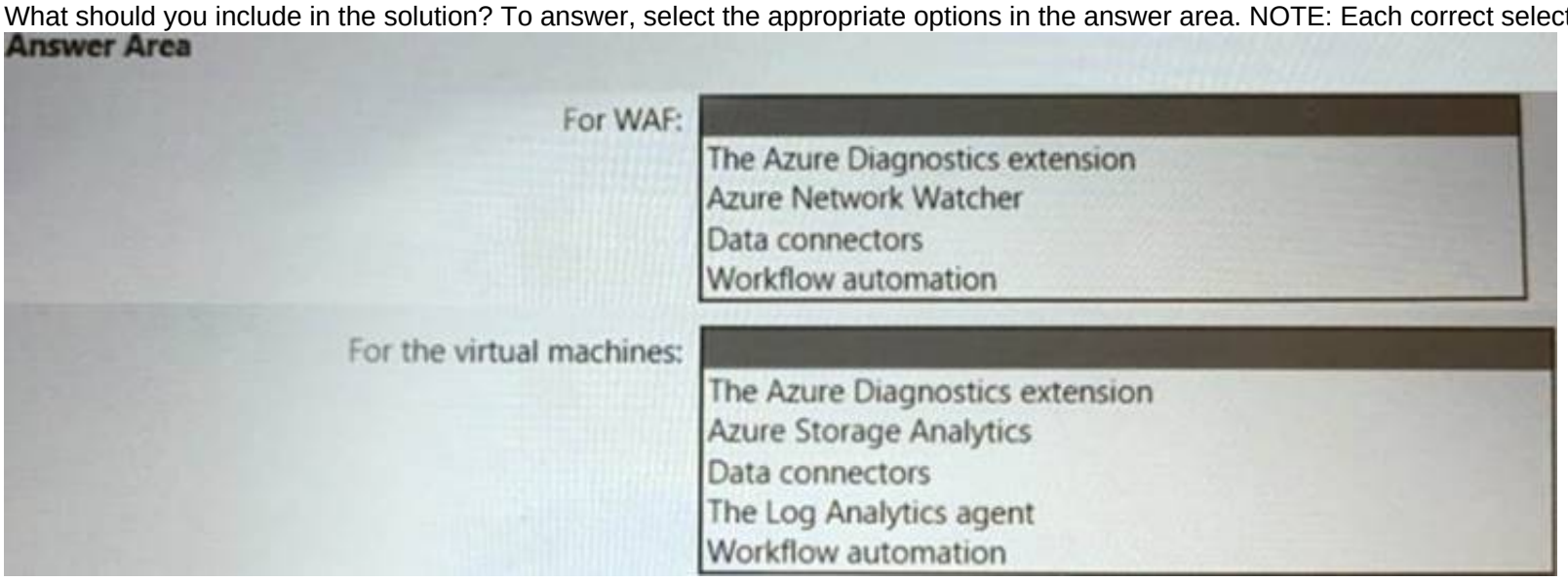
Answer: C

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

NEW QUESTION 4
- (Exam Topic 3)
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.
• Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
• Use Defender for Cloud to review alerts from the virtual machines.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

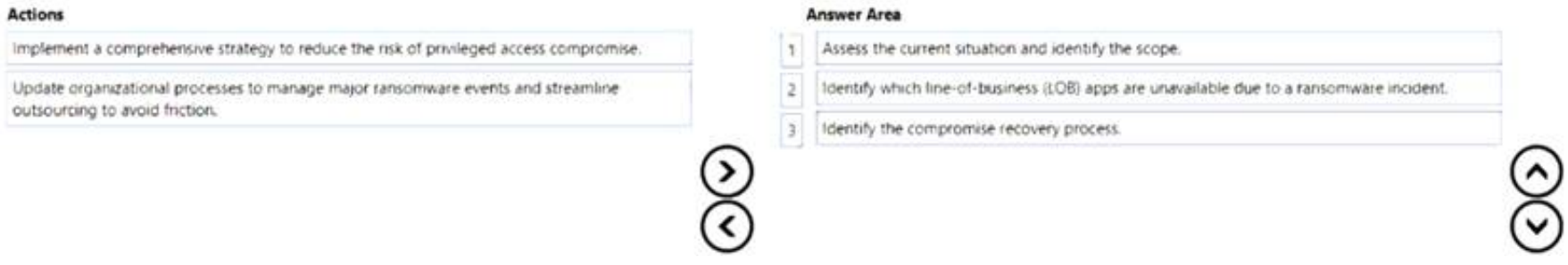
Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 5
- (Exam Topic 3)
Your company wants to optimize ransomware incident investigations.
You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.
Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 6
- (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 7
- (Exam Topic 3)
You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD)
The customer plans to obtain an Azure subscription and provision several Azure resources. You need to evaluate the customer's security environment.
What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

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

Answer: D

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

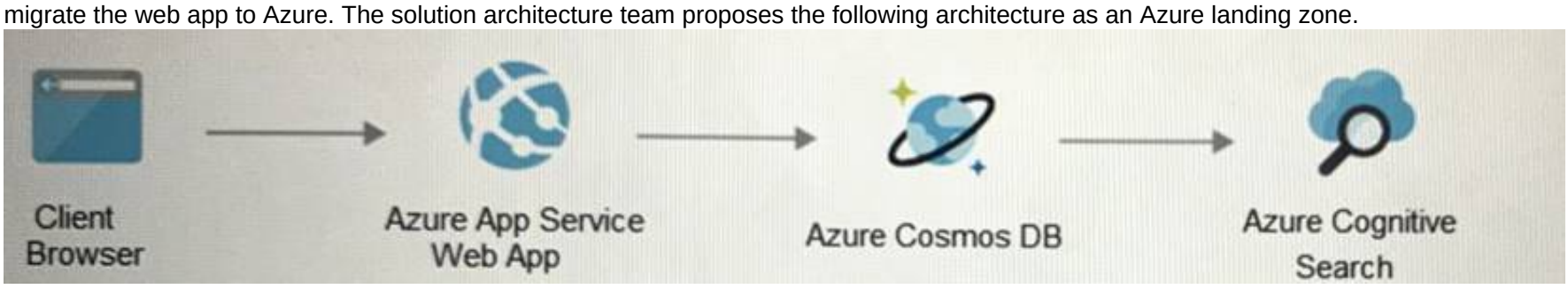
NEW QUESTION 8
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

A. Azure Monitor webhooks
B. Azure Logics Apps
C. Azure Event Hubs
D. Azure Functions apps

Answer: B

Explanation:
The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

NEW QUESTION 9
- (Exam Topic 3)
Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Key Vault to store credentials.

A. Yes
B. No

Answer: B

Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

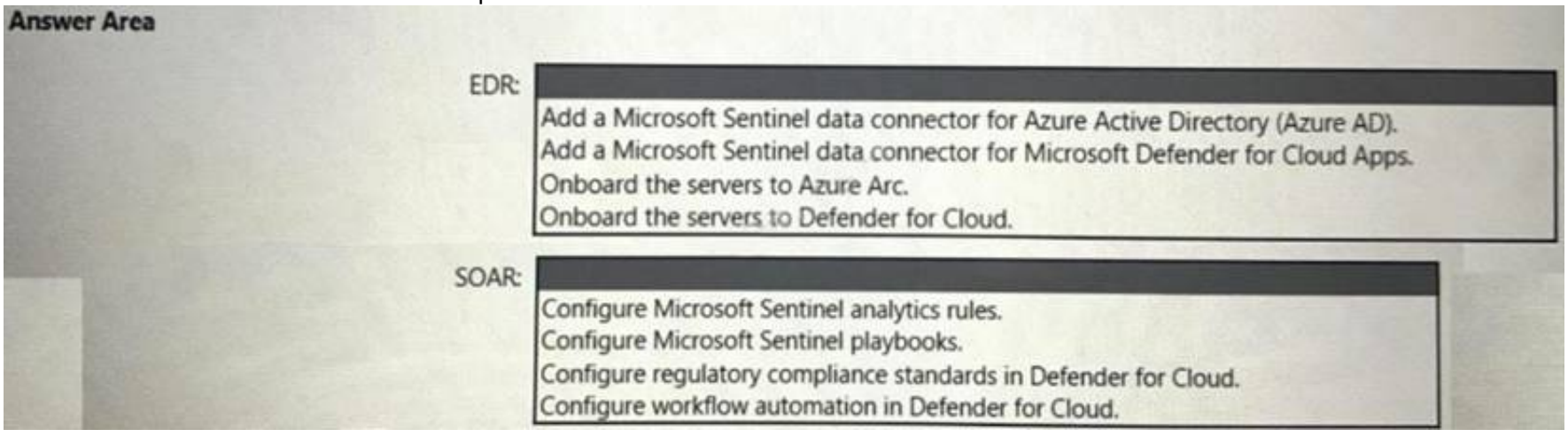
NEW QUESTION 10
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware 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)
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.

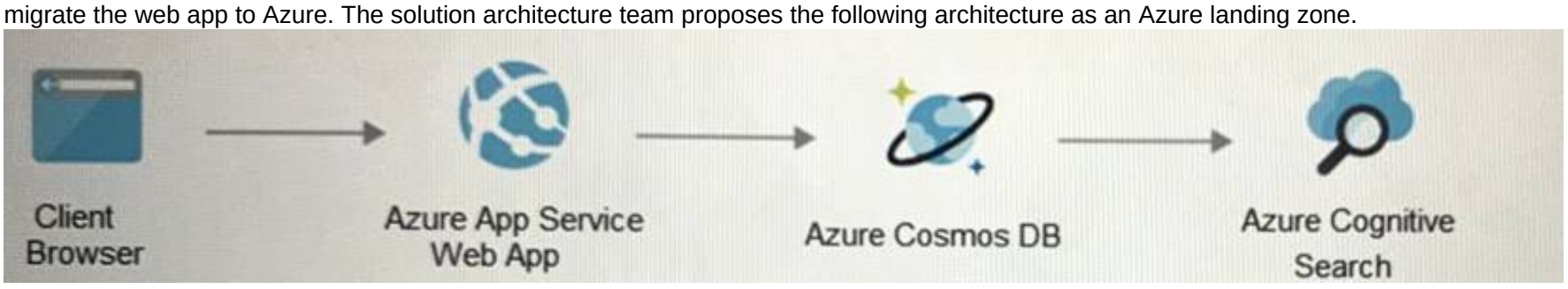


A. Mastered
B. Not Mastered

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 11
- (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 14
- (Exam Topic 3)
You are designing a ransomware response plan that follows Microsoft Security Best Practices.
You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files. What should you include in the recommendation?

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

Answer: E

NEW QUESTION 16
- (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 20
- (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 AO 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 24
- (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 25
- (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 28
- (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 30
- (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 34
- (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 38
- (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

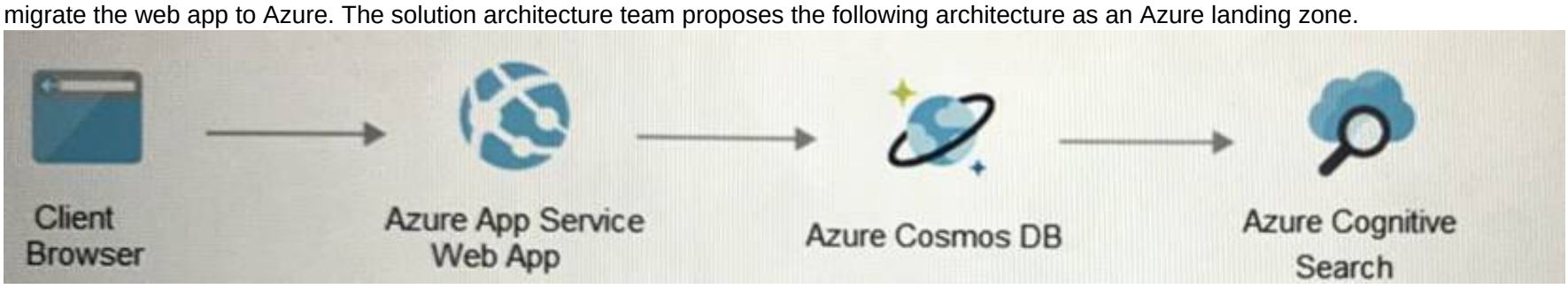
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

NEW QUESTION 43
- (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 44
- (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 47
- (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 along-side 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 48
- (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 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 50
- (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?

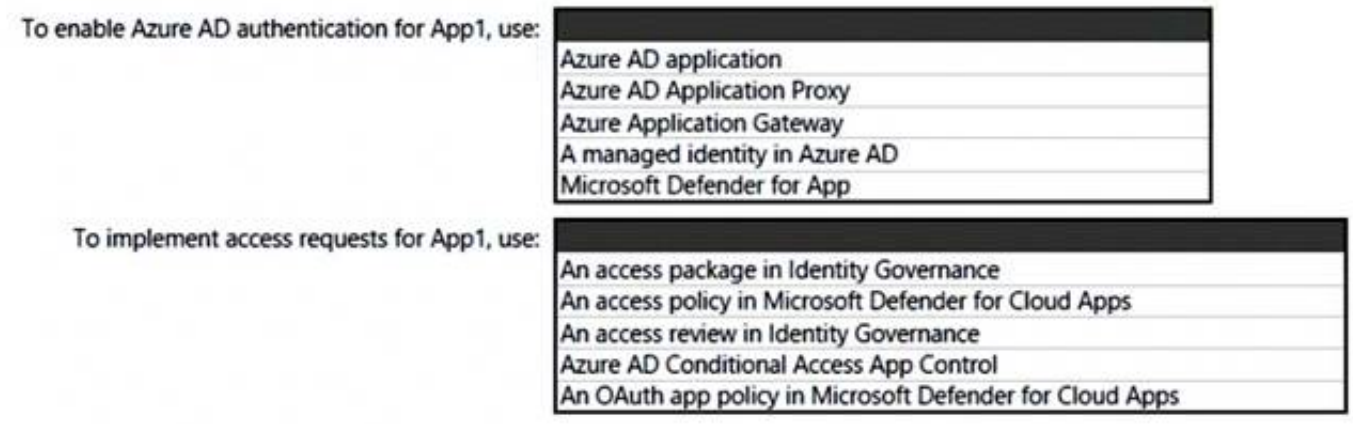
A. Microsoft Endpoint Manager
B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Answer: D

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

NEW QUESTION 53
- (Exam Topic 3)
You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:
• Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
• Users will authenticate by using Azure Active Directory (Azure AD) user accounts. You need to recommend an access security architecture for App1.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1 is the Azure AD Application
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
Box 2 is Access Package in Identity Governance
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cr

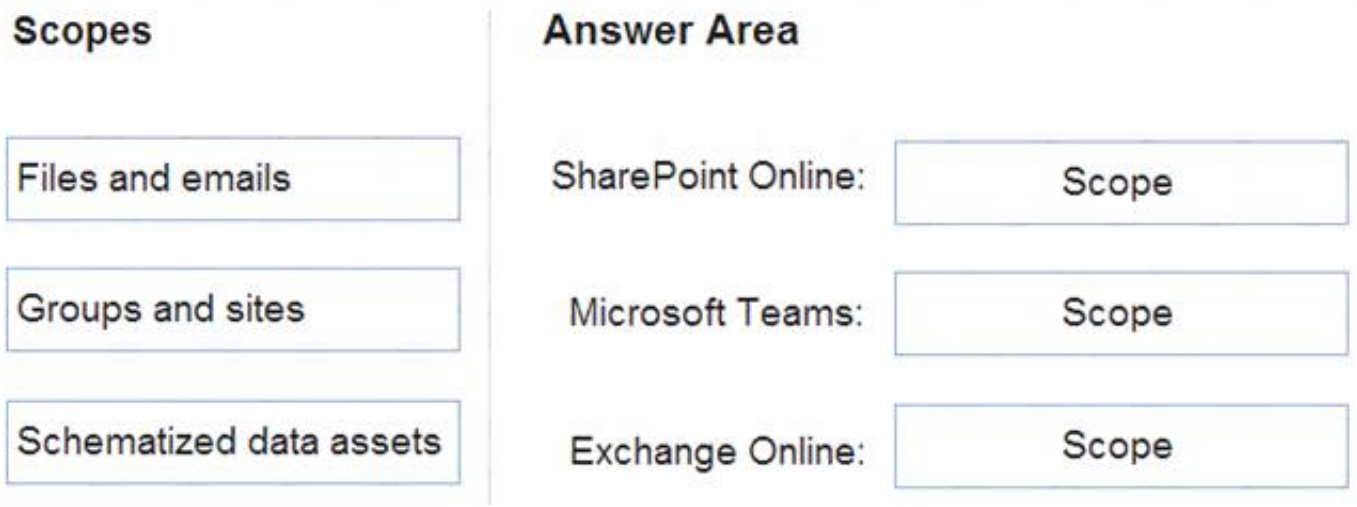
NEW QUESTION 54
- (Exam Topic 3)
Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using 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 55
- (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 56
- (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 59
- (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 62
- (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

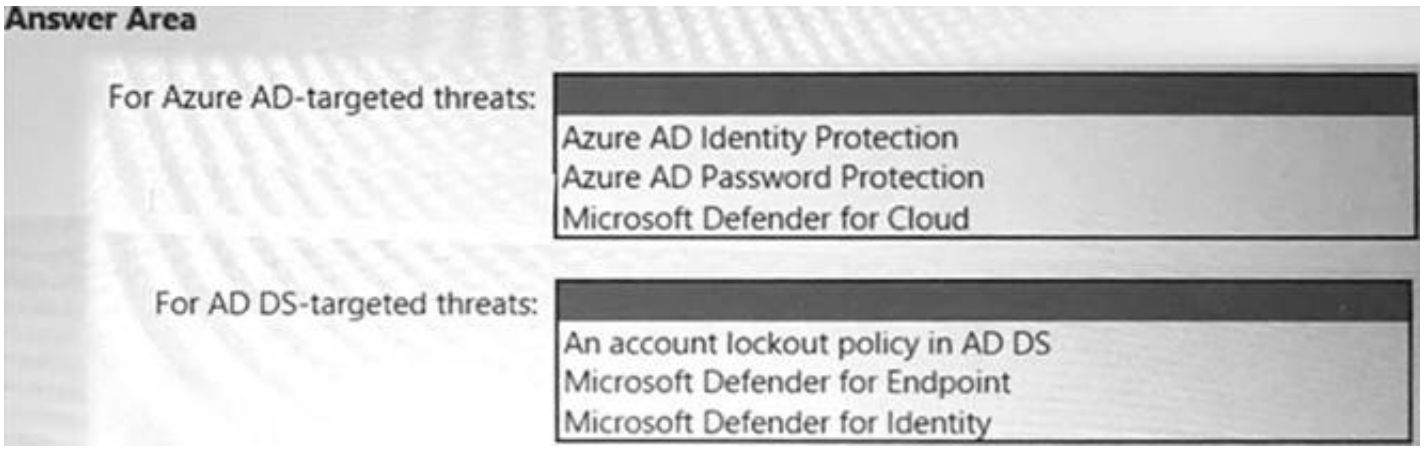
NEW QUESTION 63
- (Exam Topic 2)
To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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 65
- (Exam Topic 2)
You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE; Each correct selection is worth one point.

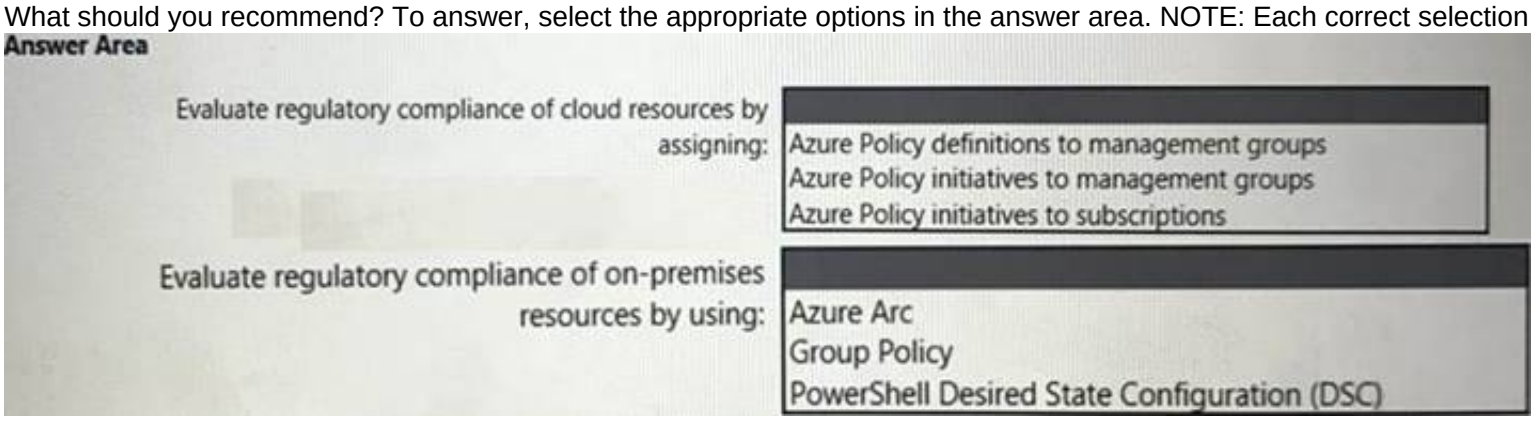


A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Azure AD Identity Protection Brute Force Detection:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
* 2. Defender for Identity
MDI can detect brute force attacks: ref:
https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts#suspected-brute-force-at

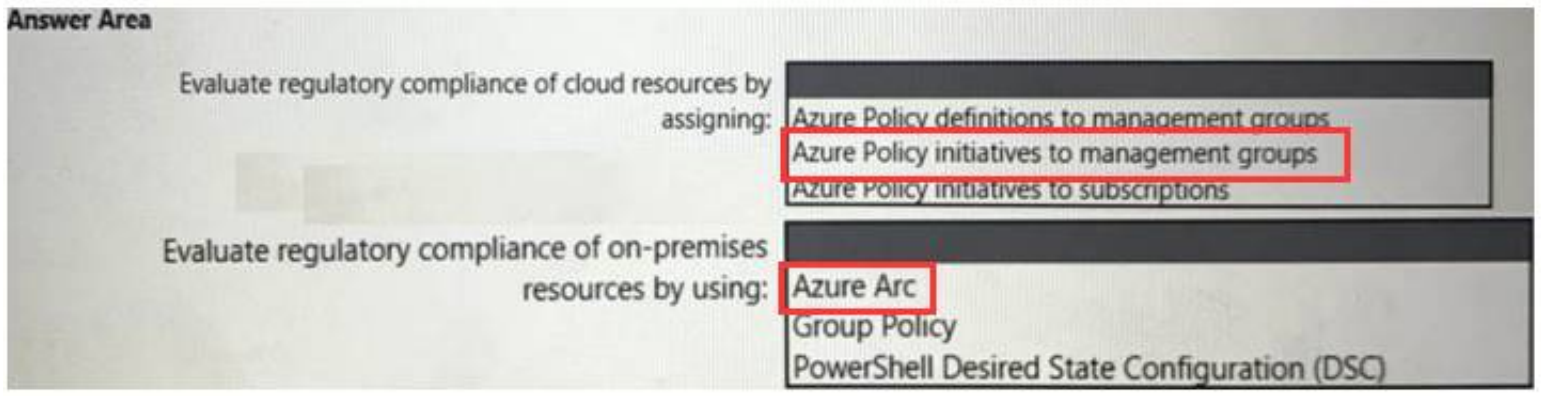
NEW QUESTION 70
- (Exam Topic 2)
You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



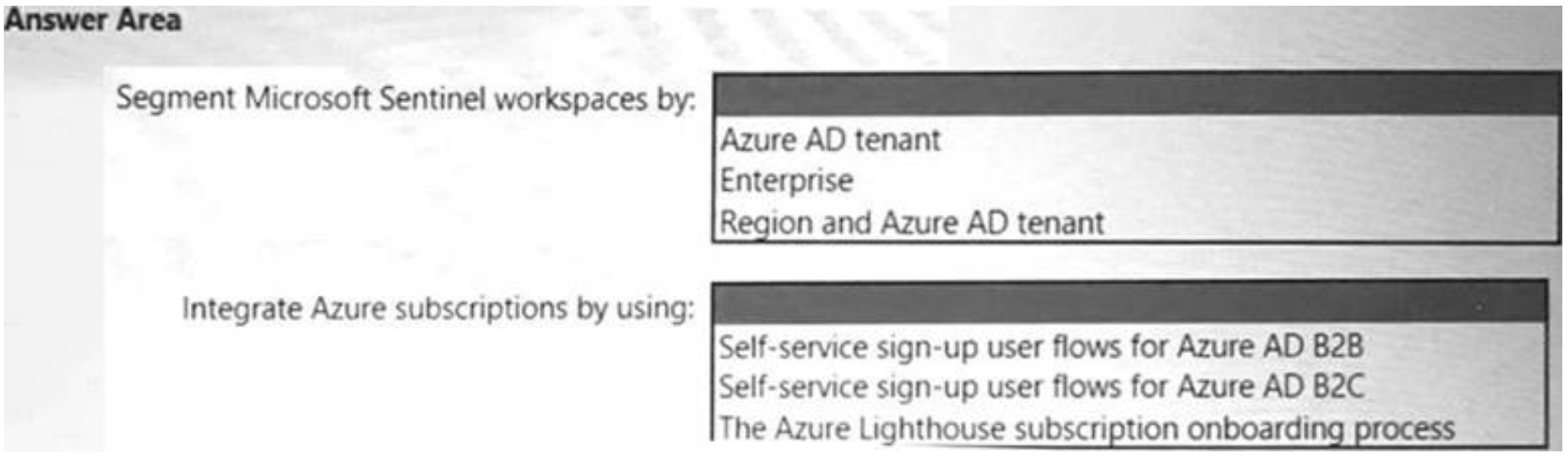
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 72
- (Exam Topic 2)
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

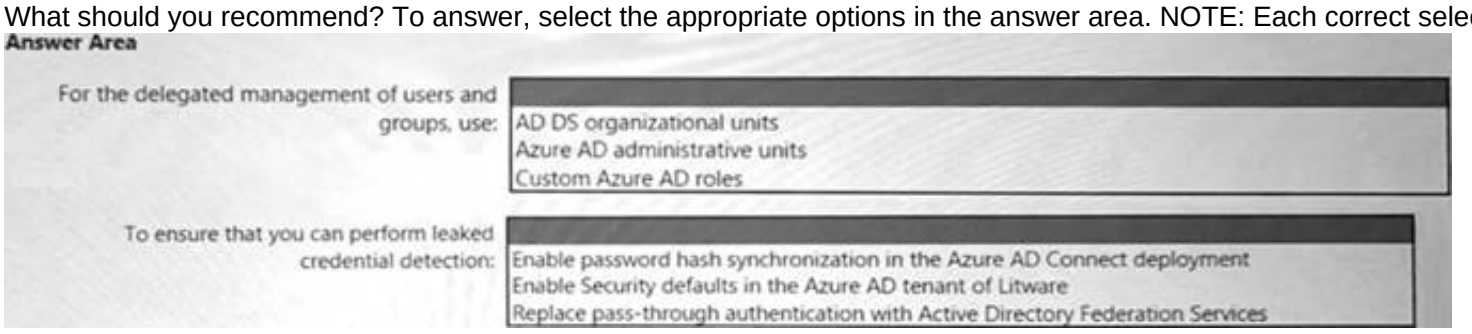
NEW QUESTION 77
- (Exam Topic 2)
You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each 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

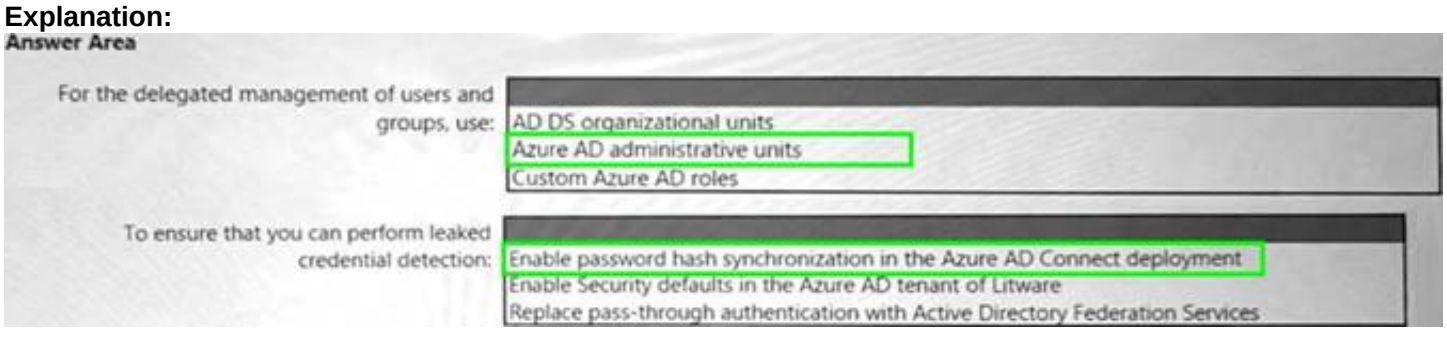
NEW QUESTION 82
- (Exam Topic 2)
You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 87
- (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

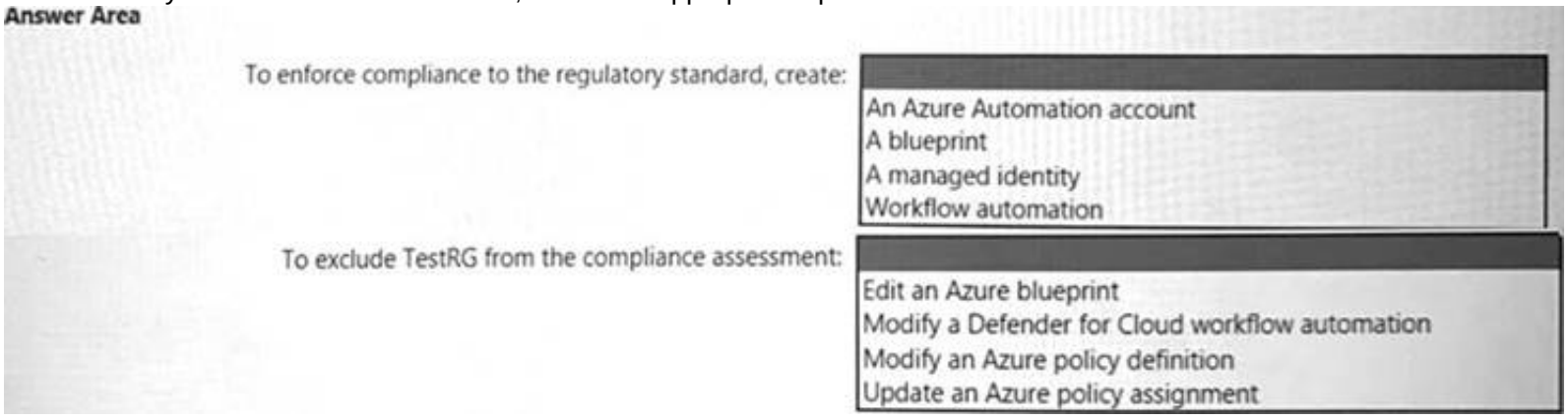
C. Application Insights in Azure Monitor
D. Azure DevTest Labs

Answer: B

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

NEW QUESTION 89
- (Exam Topic 1)
You need to recommend a solution to meet the compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1 = A Blueprint
Box 2 = Update an Azure Policy assignment
https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure
while it is in policy assignment
- https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure

NEW QUESTION 90
- (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 91
- (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 92
- (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 94
- (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 97
- (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 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps
B. adaptive application controls in Defender for Cloud
C. Azure Security Benchmark compliance controls m Defender for Cloud
D. app protection policies in Microsoft Endpoint Manager

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute-recommendati

NEW QUESTION 100
- (Exam Topic 3)
You have an Azure subscription.
You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar. Developers use Azure DevOps to deploy web apps to App Service Environments- When a new app is
deployed, a CNAME record for the app is registered in contoso.com.
You need to recommend a solution to secure the DNS record tor each web app. The solution must meet the following requirements:
• Ensure that when an app is deleted, the CNAME record for the app is removed also
• Minimize administrative effort.
What should you include in the recommendation?

A. Microsoft Defender for DevOps
B. Microsoft Defender foe App Service
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for DNS

Answer: C

NEW QUESTION 103
- (Exam Topic 3)
You have a Microsoft 365 tenant.
Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:
• Users must be able to request access to App1 by using a self-service request.
• When users request access to App1, they must be prompted to provide additional information about their request.
• Every three months, managers must verify that the users still require access to Appl. What should you include in the design?

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

Answer: C

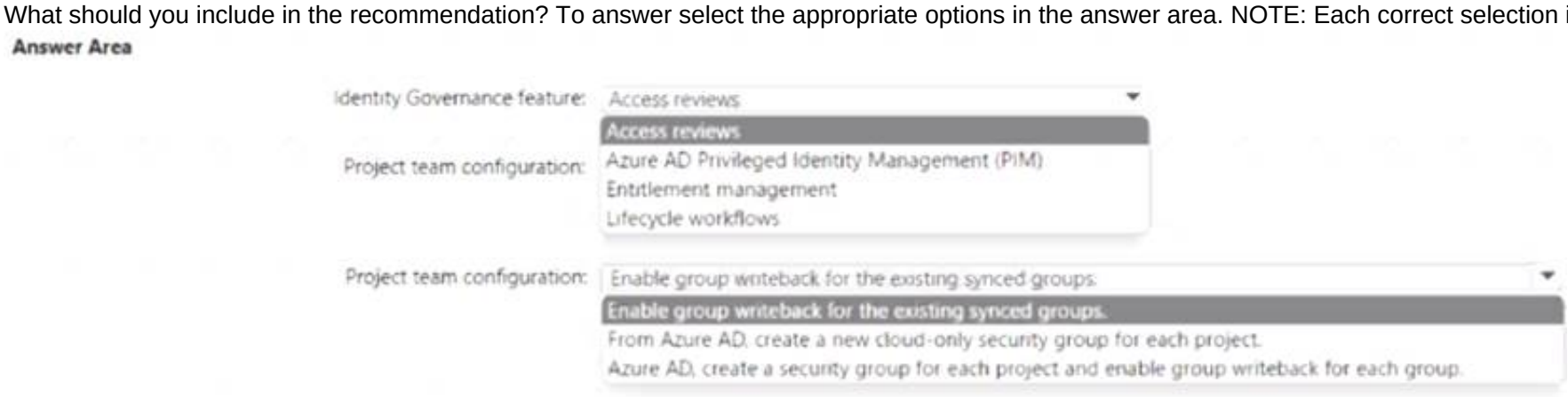
NEW QUESTION 107
- (Exam Topic 3)
You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using
continuous integration and continuous deployment (CI/CD) pipelines.

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

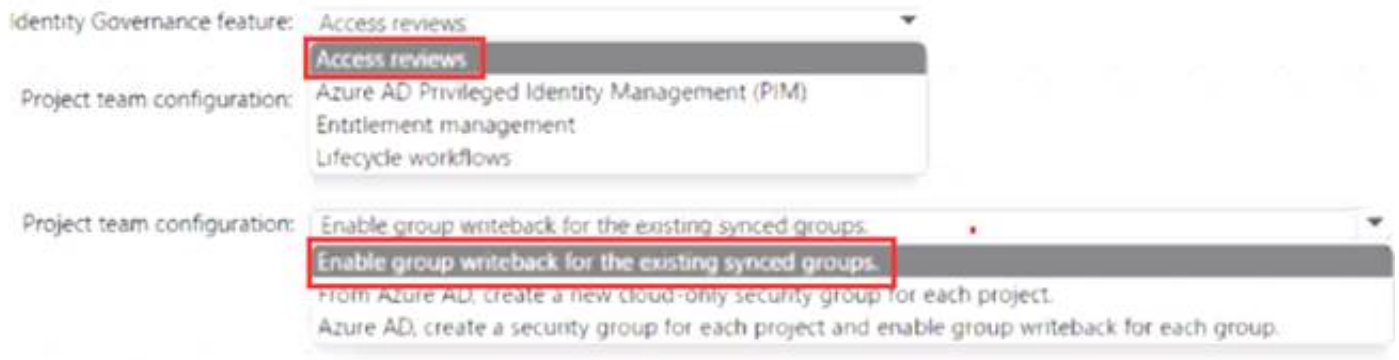
NEW QUESTION 112
- (Exam Topic 3)
Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



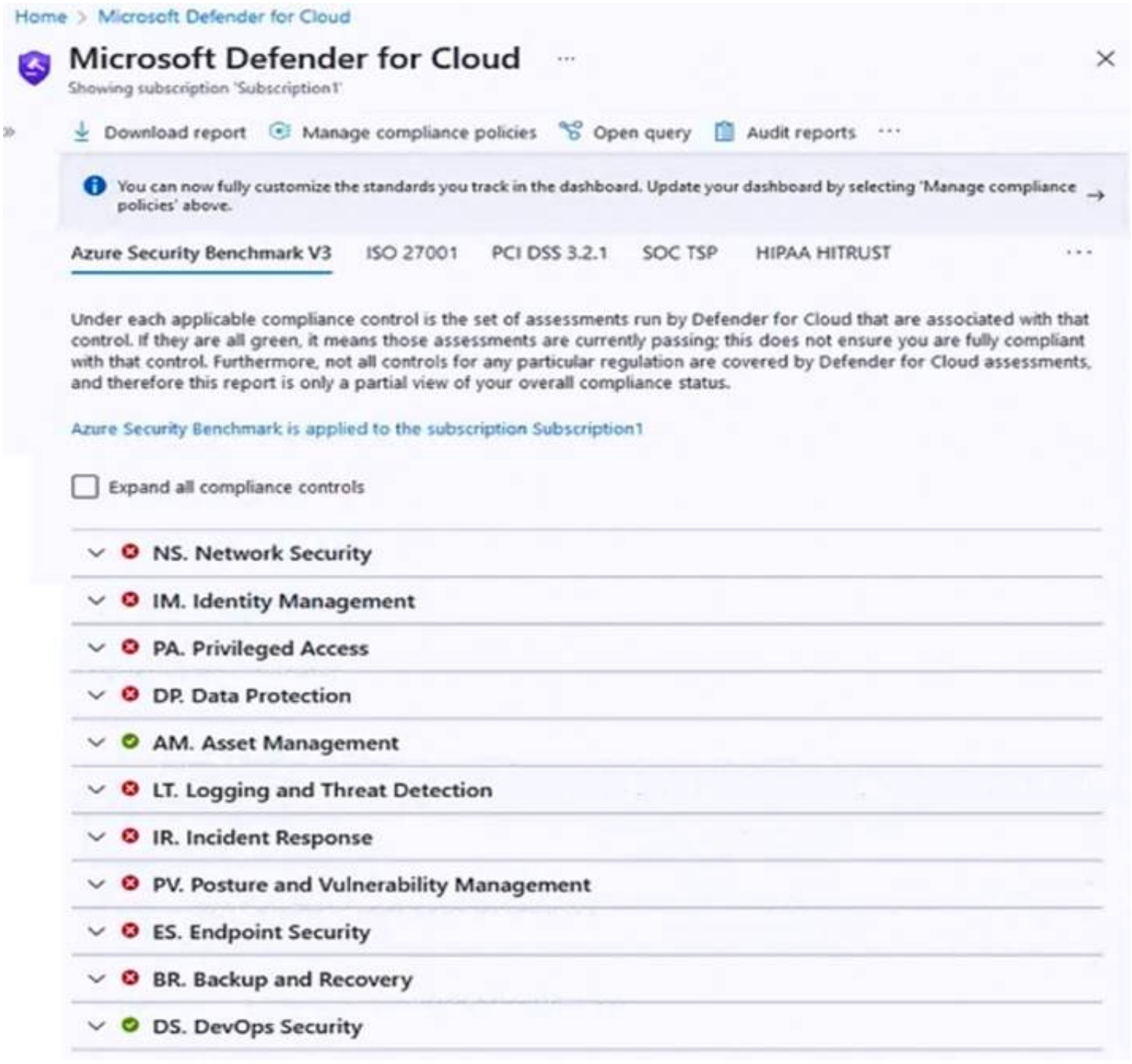
NEW QUESTION 116
- (Exam Topic 3)
Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD). You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications. What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps
B. sign-in risk policies in Azure AD Identity Protection
C. device compliance policies in Microsoft Endpoint Manager
D. Azure AD Conditional Access policies
E. user risk policies in Azure AD Identity Protection

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-loca https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules

NEW QUESTION 117
- (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 122
- (Exam Topic 3)
Your company plans to provision blob storage by using an Azure Storage account The blob storage will be accessible from 20 application sewers on the internet. You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

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

Answer: D

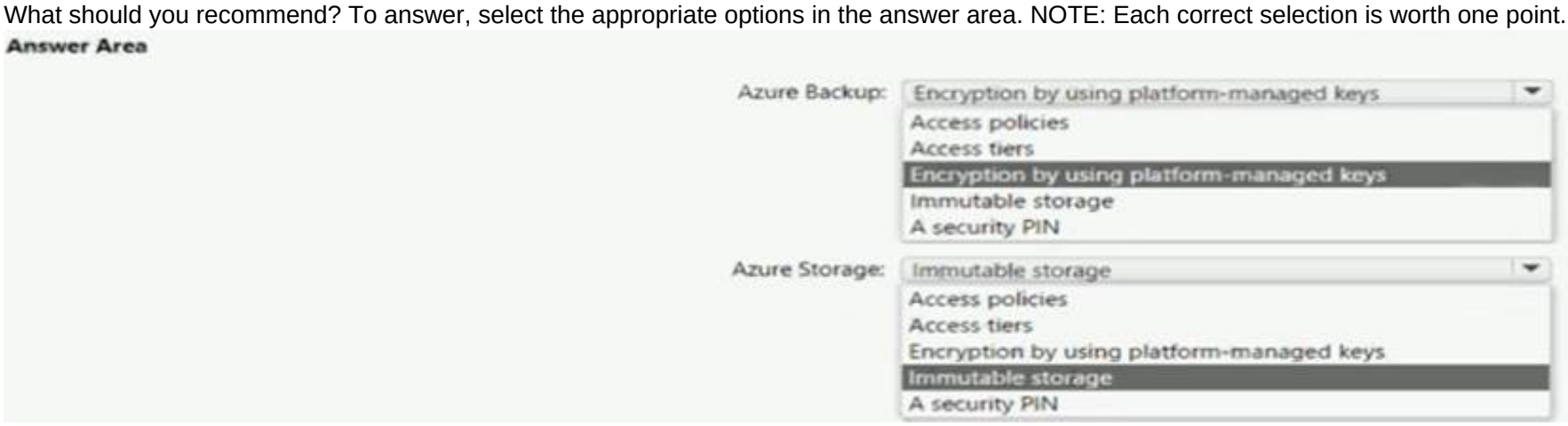
NEW QUESTION 125
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

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.

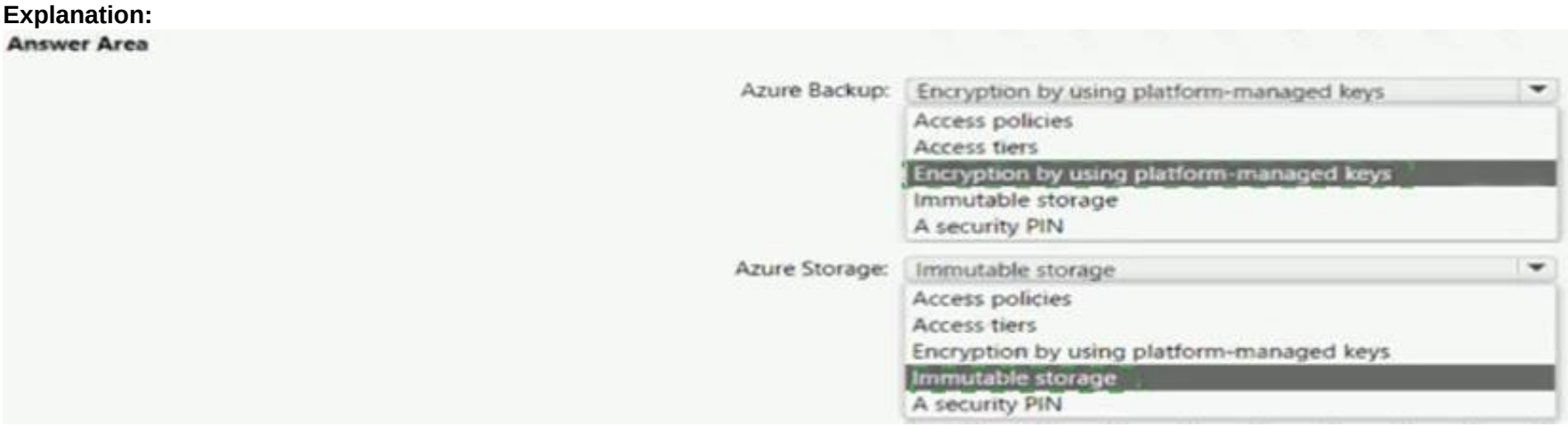
NEW QUESTION 128
- (Exam Topic 3)
Your company wants to optimize using Azure to protect its resources from ransomware.
You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



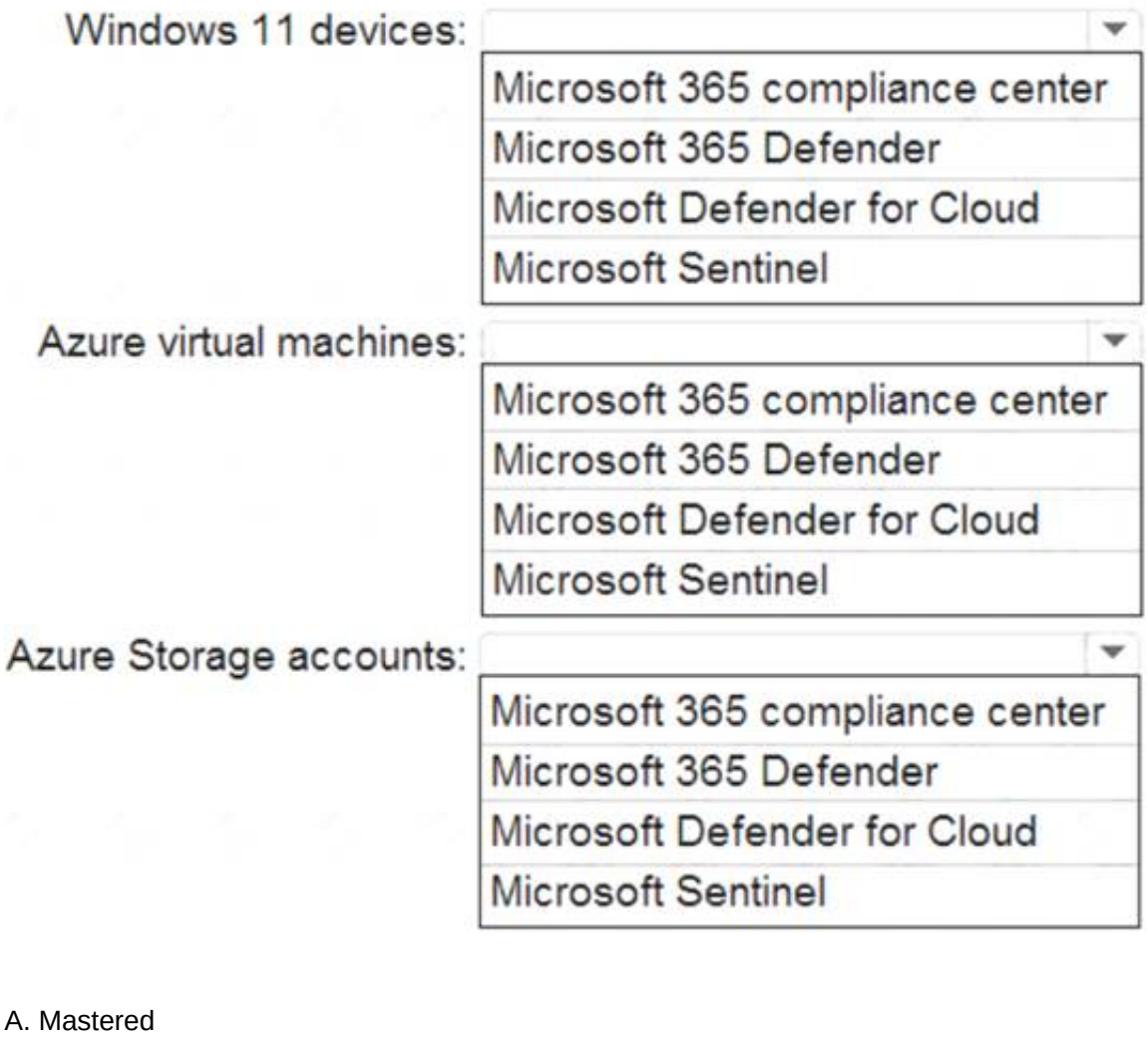
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 132
- (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 135
- (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 137
- (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:

NEW QUESTION 140
- (Exam Topic 3)
You have legacy operational technology (OT) devices and IoT devices.
You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures (MCRA). The solution must minimize the risk of disrupting business operations.
Which two security methodologies should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point

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

Answer: CD

NEW QUESTION 142
- (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.

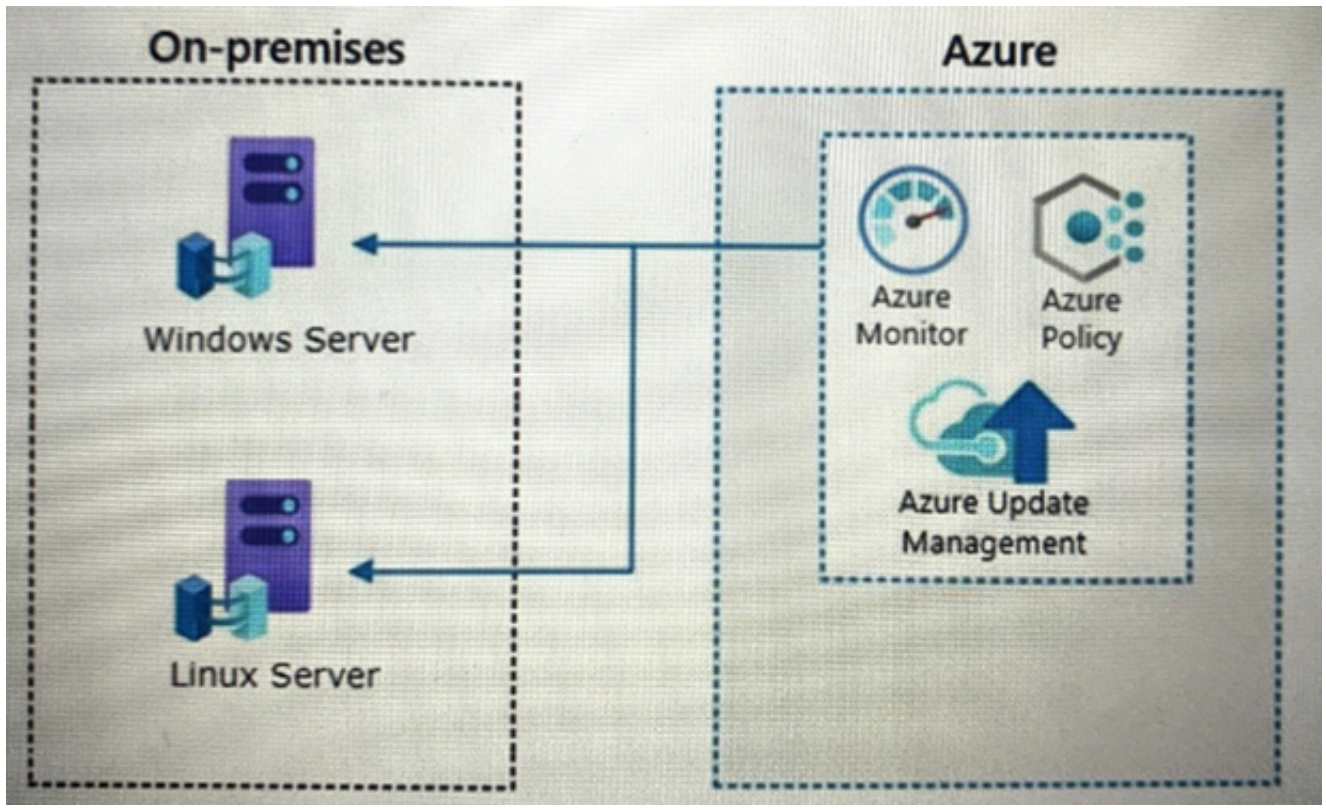
Answer: AD

NEW QUESTION 146
- (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 148
- (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

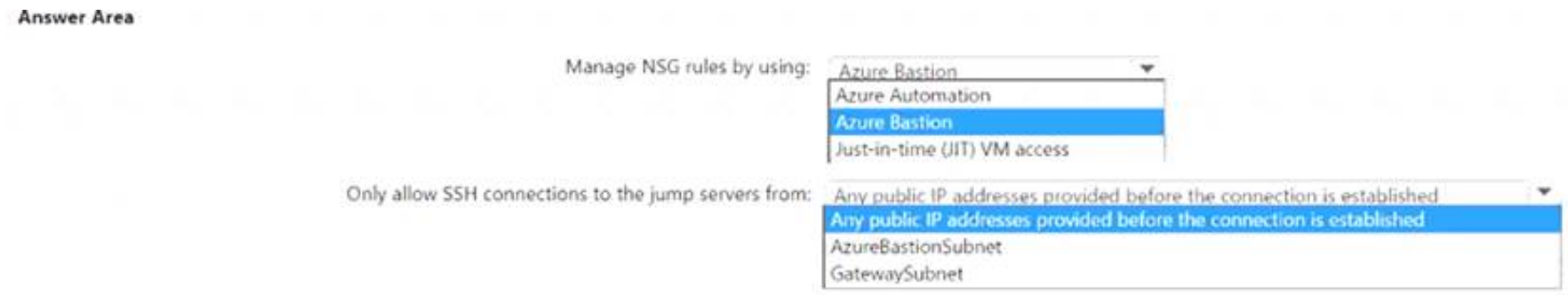
NEW QUESTION 149
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
• Identify unused personal data and empower users to make smart data handling decisions.
• Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
• Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

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

Answer: C

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

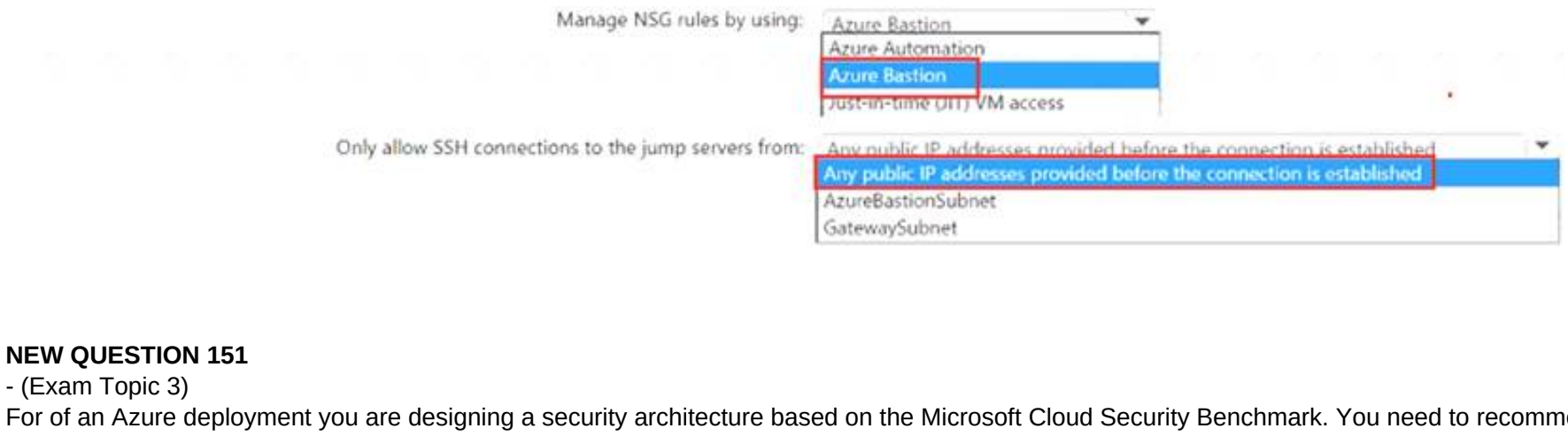
NEW QUESTION 150
- (Exam Topic 3)
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

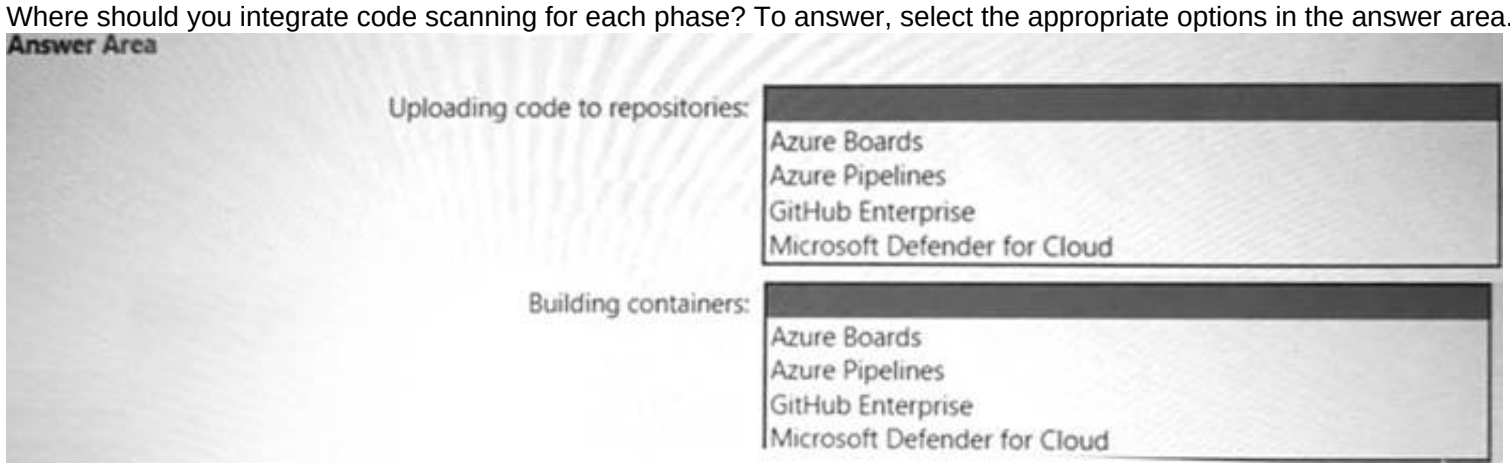


NEW QUESTION 151
- (Exam Topic 3)
For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management What should you include in the recommendation?

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

Answer: E

NEW QUESTION 156
- (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 161
- (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 164
- (Exam Topic 3)
Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks. The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:
• Prevent exposing the public IP addresses of the virtual machines.
• Provide the ability to connect without using a VPN.
• Minimize costs.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AD

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

NEW QUESTION 168
- (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

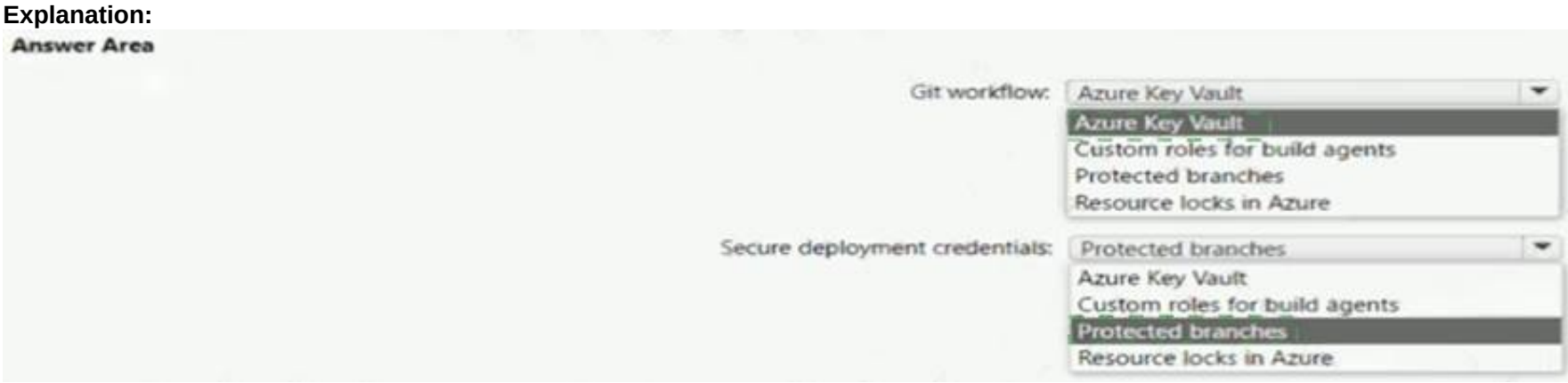
Explanation:
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-acc

NEW QUESTION 173
- (Exam Topic 3)
You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CO) workflows.
You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.
What should you include in the recommendation for each stage? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 178
- (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:

NEW QUESTION 179
- (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 183
- (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 186
- (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.

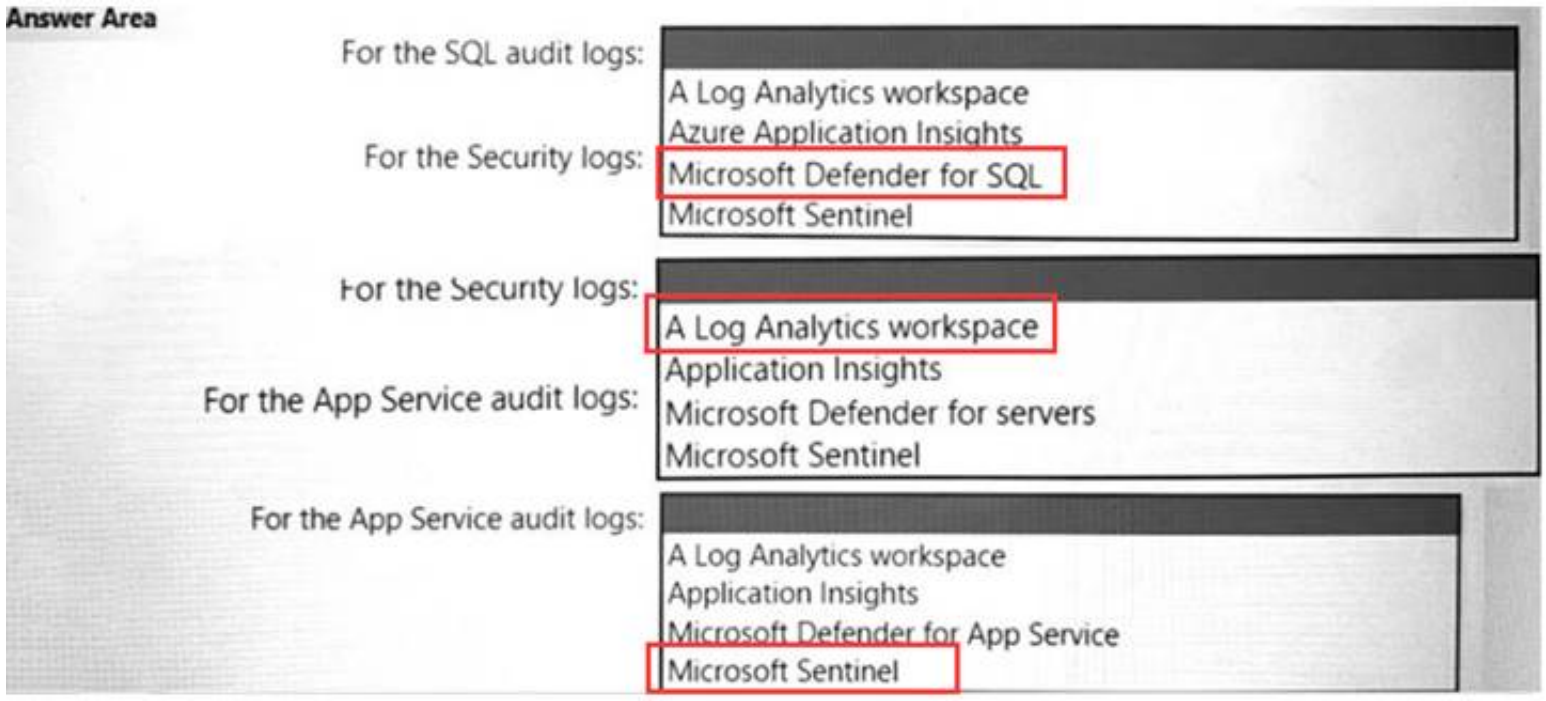
Answer: C

NEW QUESTION 187
- (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.

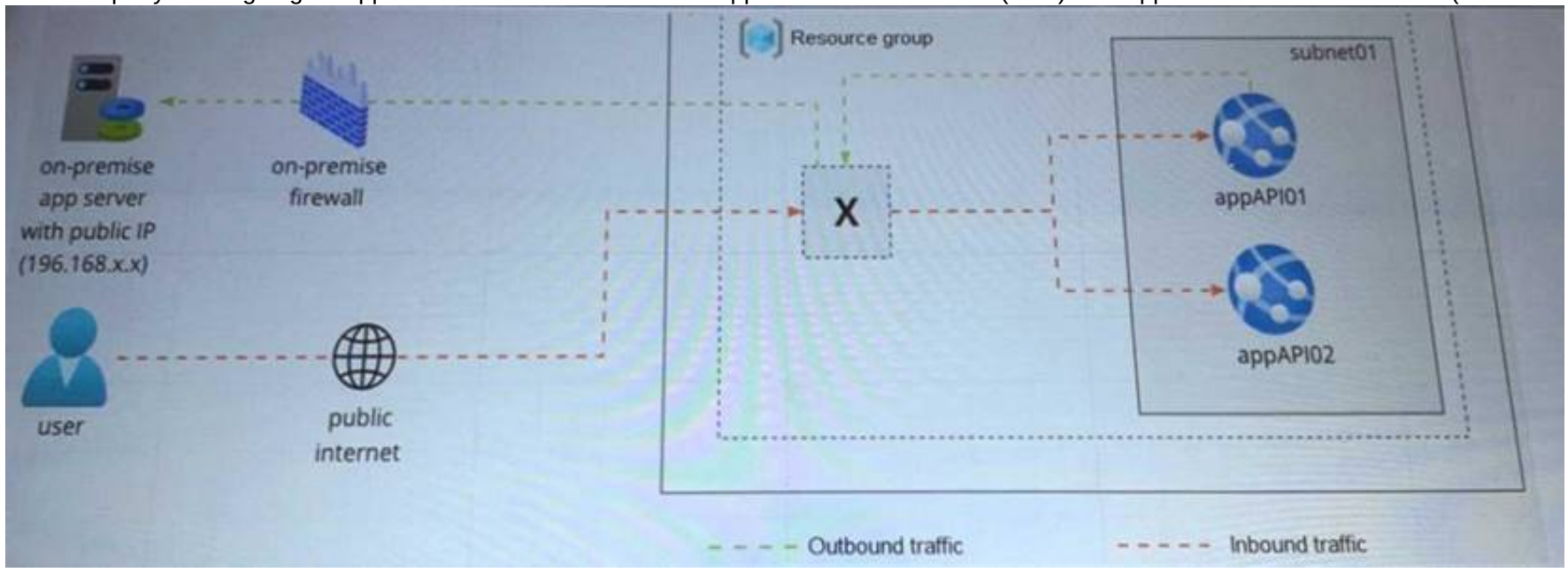
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 192
- (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 195
- (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 198
- (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 200
.....

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