Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1
- (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

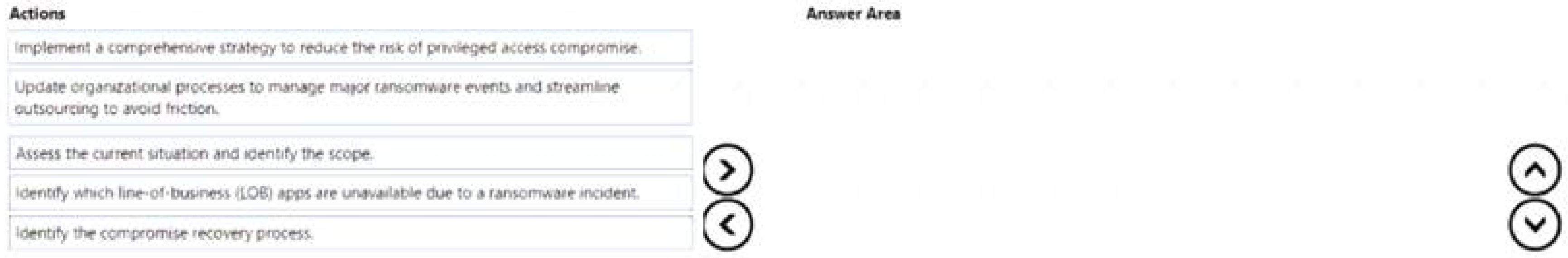
NEW QUESTION 2
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions that allow traffic from the Front Door service tags. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 3
- (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.



Implement a comprehensive strategy to reduce the risk of privileged access compromise.

Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

Assess the current situation and identify the scope.

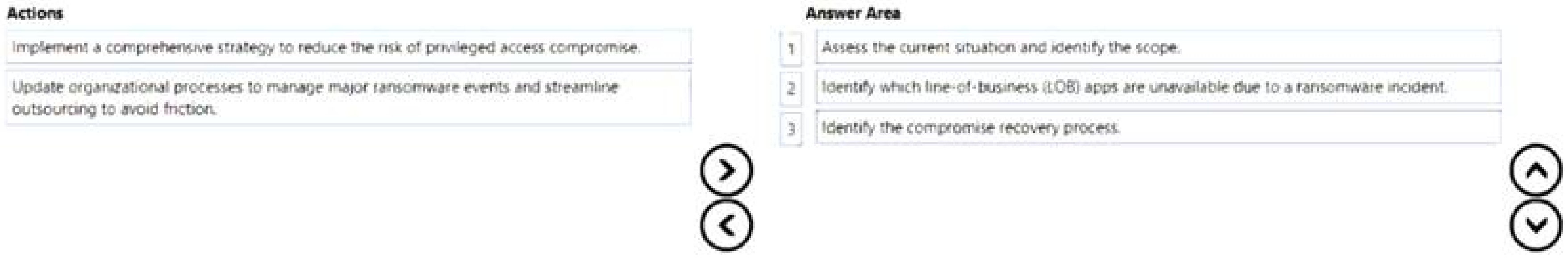
Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.

Identify the compromise recovery process.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Implement a comprehensive strategy to reduce the risk of privileged access compromise.

Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

1 Assess the current situation and identify the scope.

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

3 Identify the compromise recovery process.

NEW QUESTION 4
- (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 5
- (Exam Topic 3)
You have a Microsoft 365 subscription.
You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.
Which two services should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 6
- (Exam Topic 3)
You have 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 7
- (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

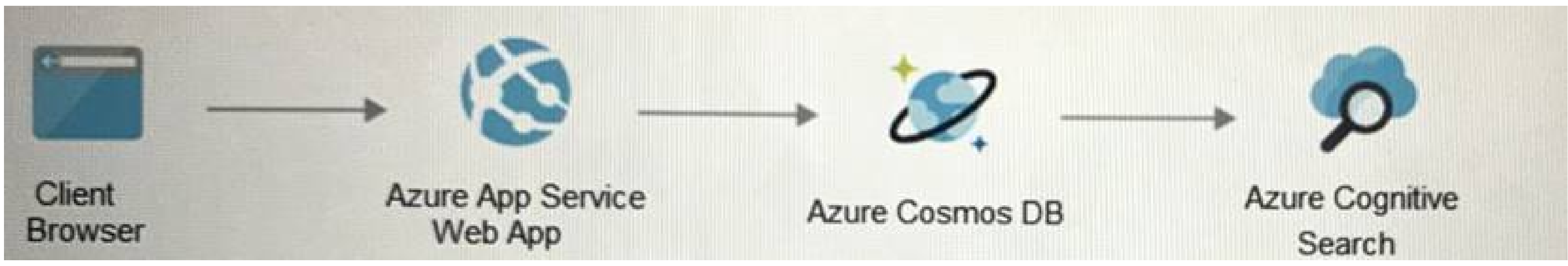
NEW QUESTION 8
- (Exam Topic 3)
You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements.
What should you recommend as part of the landing zone deployment?

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

Answer: A

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

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



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes
B. No

Answer: B

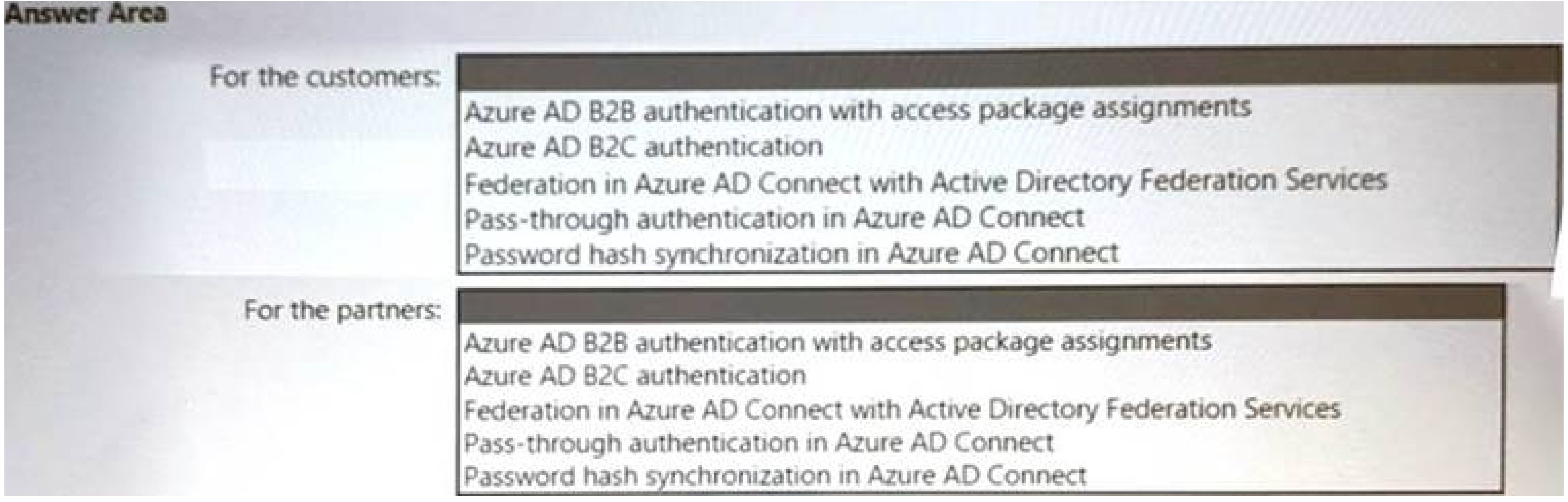
Explanation:
https://www.varonis.com/blog/securing-access-azure-webapps

NEW QUESTION 10
- (Exam Topic 3)
Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure.
You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure.
What should you use to start the threat modeling process?

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

Answer: C

NEW QUESTION 10
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DSV You need to recommend an identity security strategy that meets the following requirements:
• Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website
• Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned
The solution must minimize the need to deploy additional infrastructure components. What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

For the customers:
Azure AD B2B authentication with access package assignments
Azure AD B2C authentication
Federation in Azure AD Connect with Active Directory Federation Services
Pass-through authentication in Azure AD Connect
Password hash synchronization in Azure AD Connect

For the partners:
Azure AD B2B authentication with access package assignments
Azure AD B2C authentication
Federation in Azure AD Connect with Active Directory Federation Services
Pass-through authentication in Azure AD Connect
Password hash synchronization in Azure AD Connect

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated
Box 1 --> https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview
Box 2 -- > https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers

NEW QUESTION 12
- (Exam Topic 3)
You have Microsoft Defender for Cloud assigned to Azure management groups. You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. workload protections in Defender for Cloud
B. threat intelligence reports in Defender for Cloud
C. Microsoft Sentinel notebooks
D. Microsoft Sentinel threat intelligence workbooks

Answer: BD

Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION 14
- (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

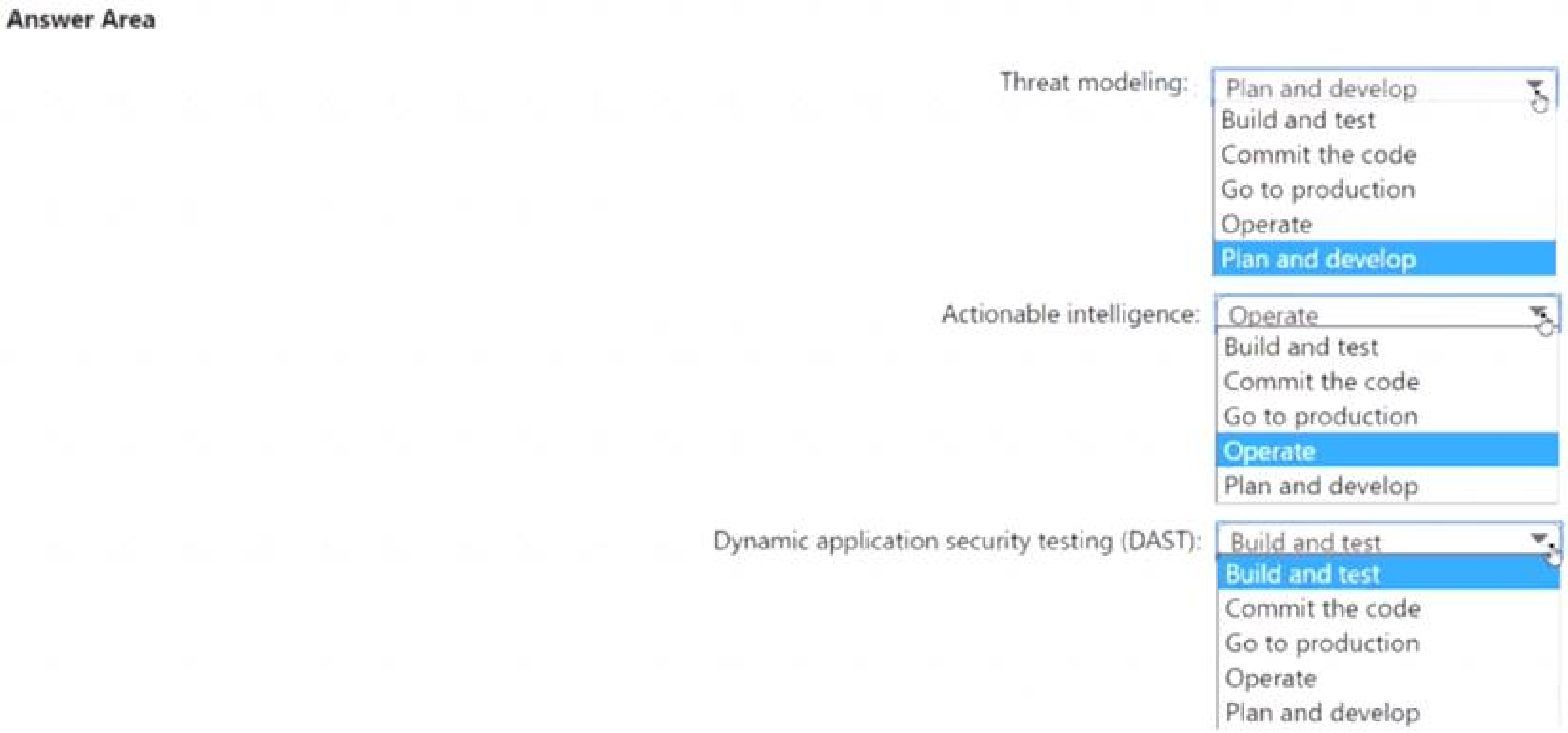
NEW QUESTION 17
- (Exam Topic 3)
You are designing the security standards for a new Azure environment.
You need to design a privileged identity strategy based on the Zero Trust model. Which framework should you follow to create the design?

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 18
- (Exam Topic 3)
You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.
During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point



Answer Area

Threat modeling: Plan and develop

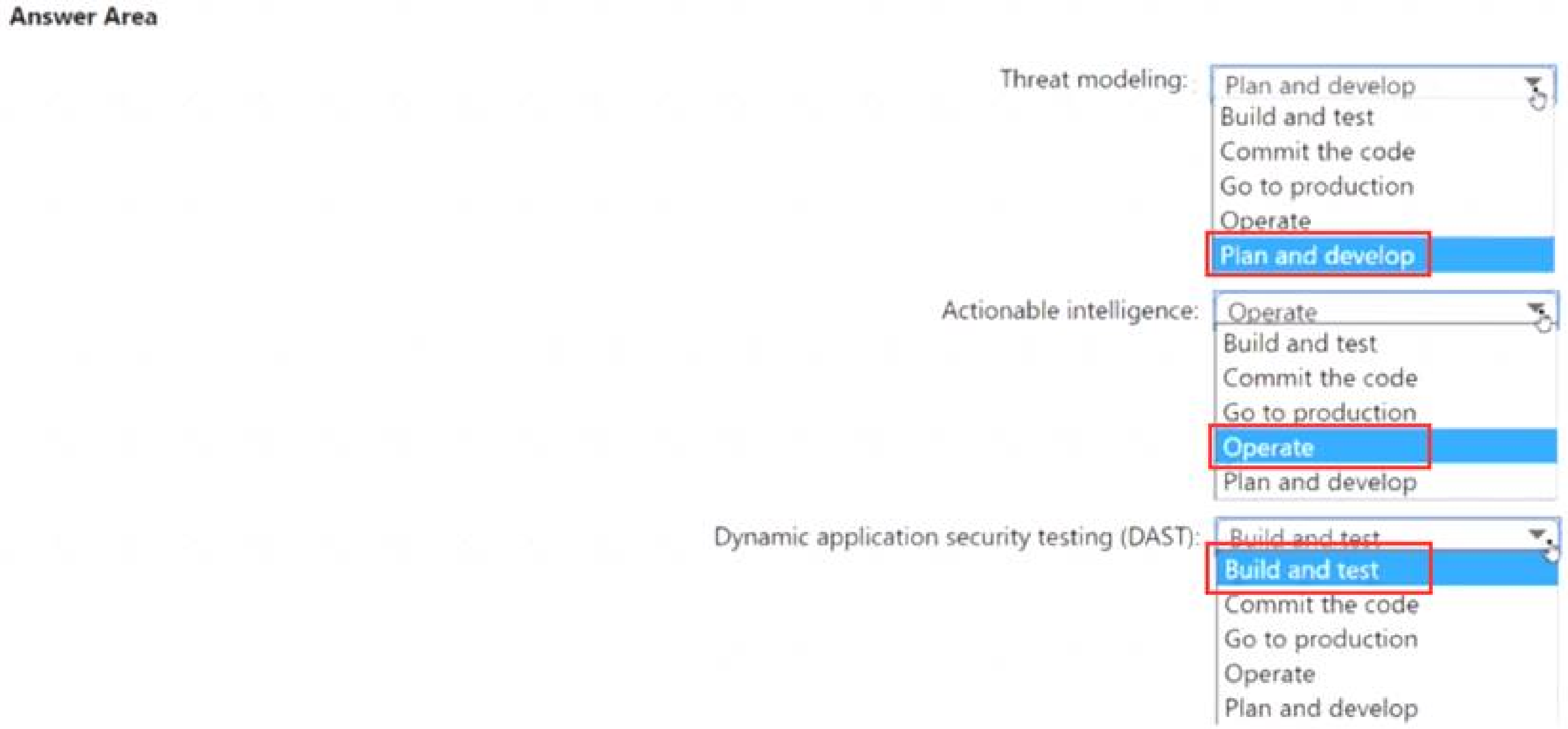
Actionable intelligence: Operate

Dynamic application security testing (DAST): Build and test

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Answer Area

Threat modeling: Plan and develop
Build and test
Commit the code
Go to production
Operate
Plan and develop

Actionable intelligence: Operate
Build and test
Commit the code
Go to production
Operate
Plan and develop

Dynamic application security testing (DAST): Build and test
Build and test
Commit the code
Go to production
Operate
Plan and develop

NEW QUESTION 20

- (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 23

- (Exam Topic 3)

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

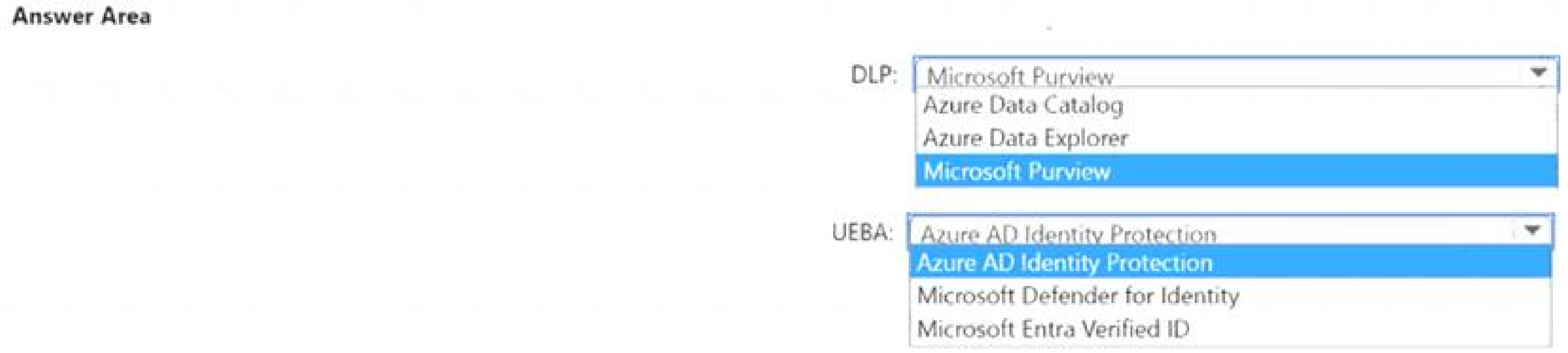
You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

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

• Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.

• Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

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


Answer Area

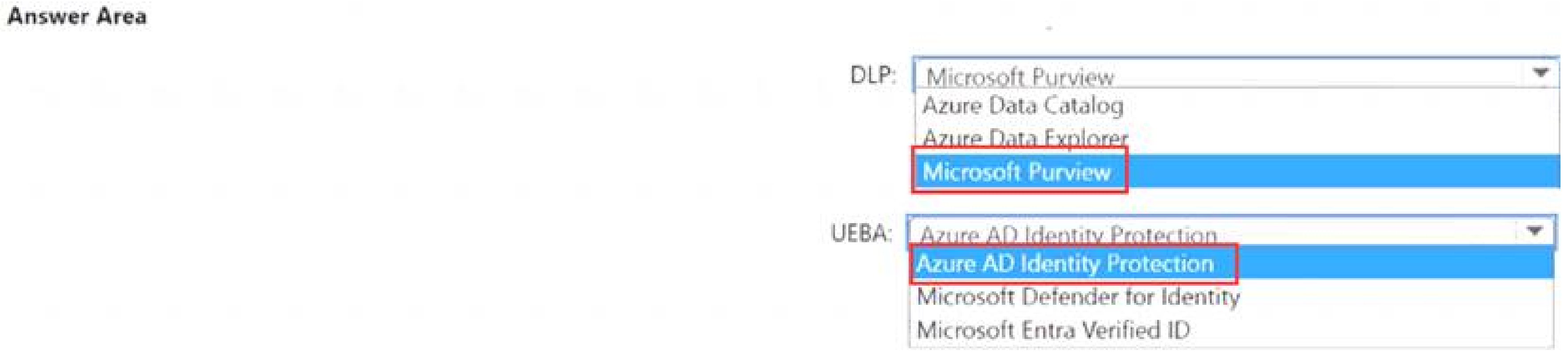
DLP: Microsoft Purview
Azure Data Catalog
Azure Data Explorer
Microsoft Purview

UEBA: Azure AD Identity Protection
Azure AD Identity Protection
Microsoft Defender for Identity
Microsoft Entra Verified ID

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Answer Area

DLP: Microsoft Purview
Azure Data Catalog
Azure Data Explorer
Microsoft Purview

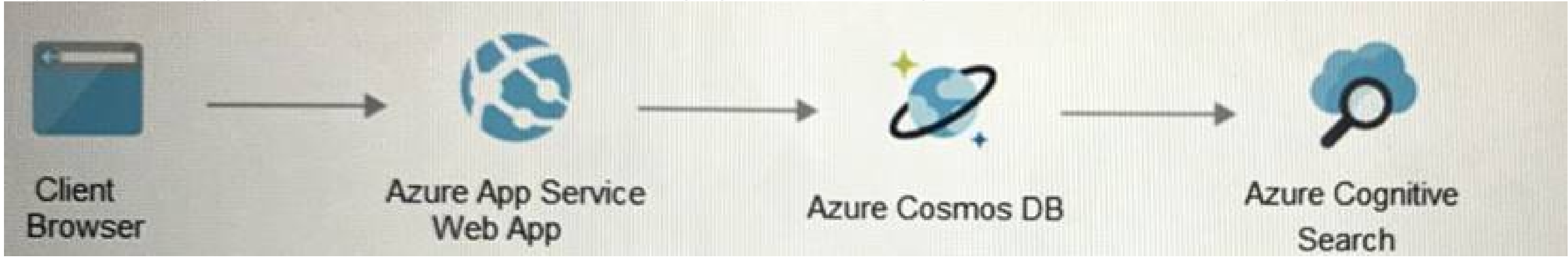
UEBA: Azure AD Identity Protection
Azure AD Identity Protection
Microsoft Defender for Identity
Microsoft Entra Verified ID

NEW QUESTION 27
- (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 32
- (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 37
- (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. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/sele

NEW QUESTION 39
- (Exam Topic 3)
Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.
You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
What should you recommend?

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

Answer: D

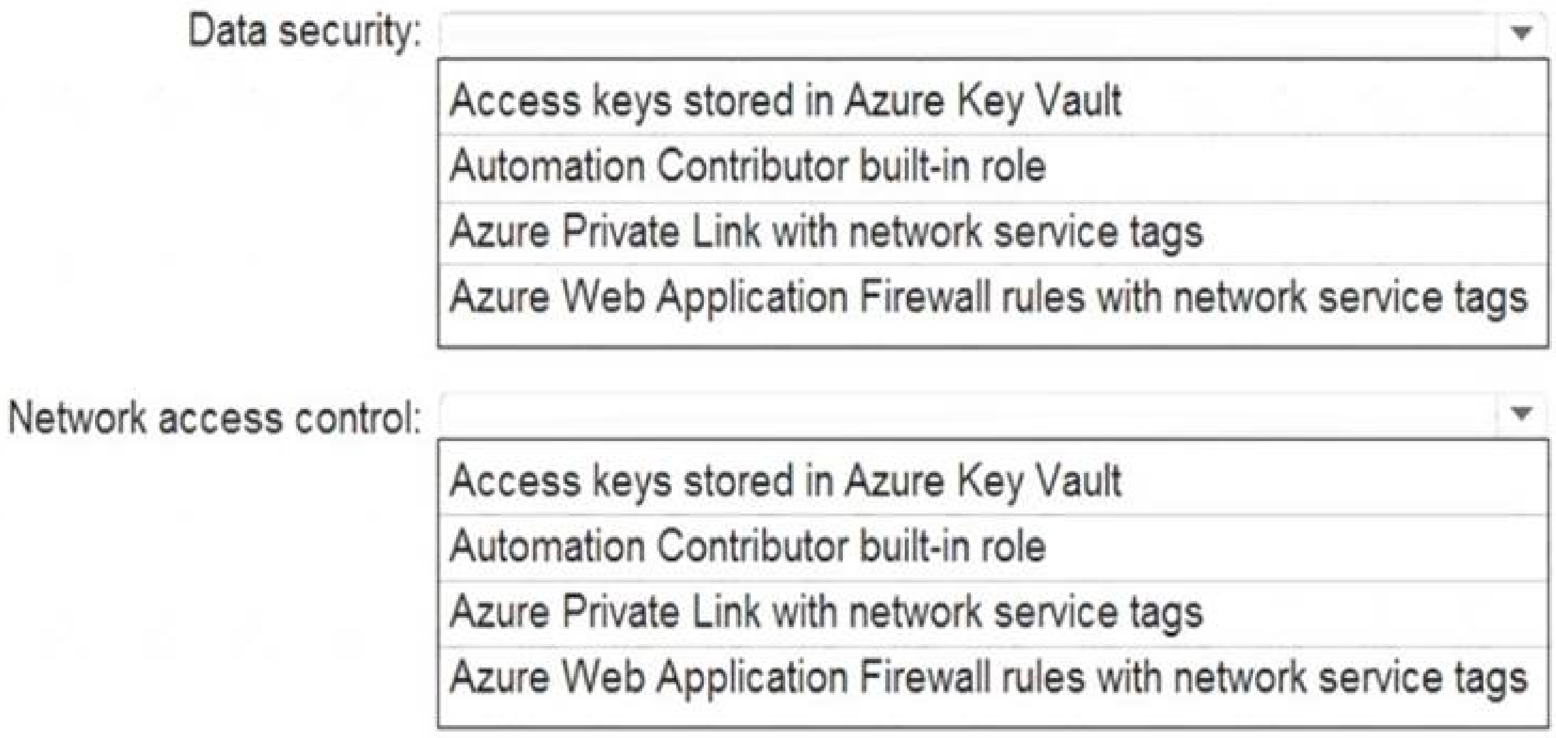
NEW QUESTION 41
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 46
- (Exam Topic 3)
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.
You need to recommend a solution to secure the components of the copy process.
What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Data security:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

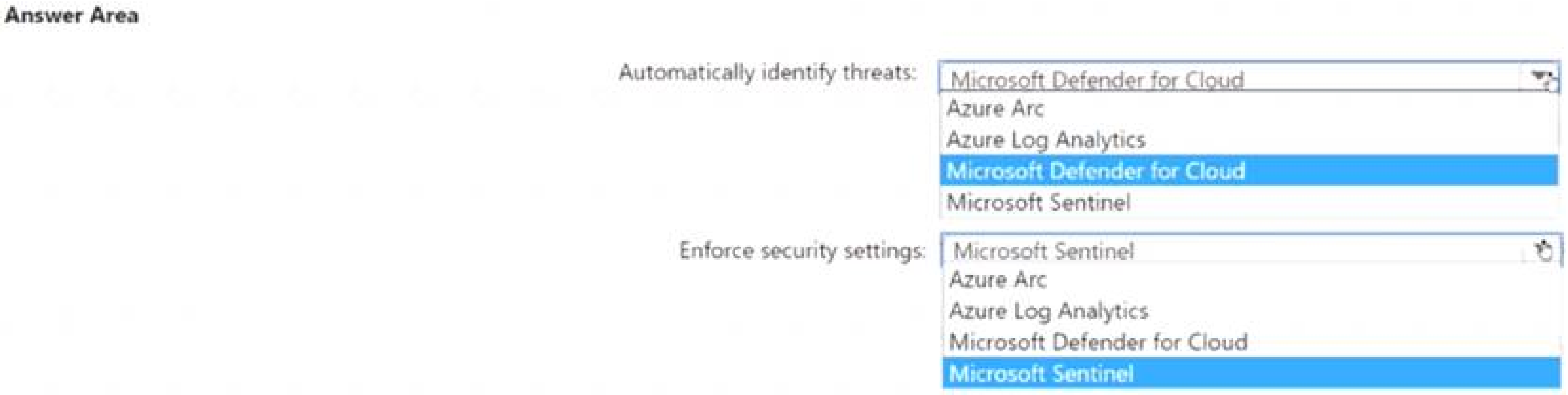
Network access control:
- Access keys stored in Azure Key Vault
- Automation Contributor built-in role
- Azure Private Link with network service tags
- Azure Web Application Firewall rules with network service tags

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Data Security = Access Keys stored in Azure Key Vault
Network access control = Azure Private Link with network service tags
https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security

NEW QUESTION 51
- (Exam Topic 3)
You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.
You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:
• Automatically identify threats found in AWS CloudTrail events.
• Enforce security settings on AWS virtual machines by using Azure policies.
What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

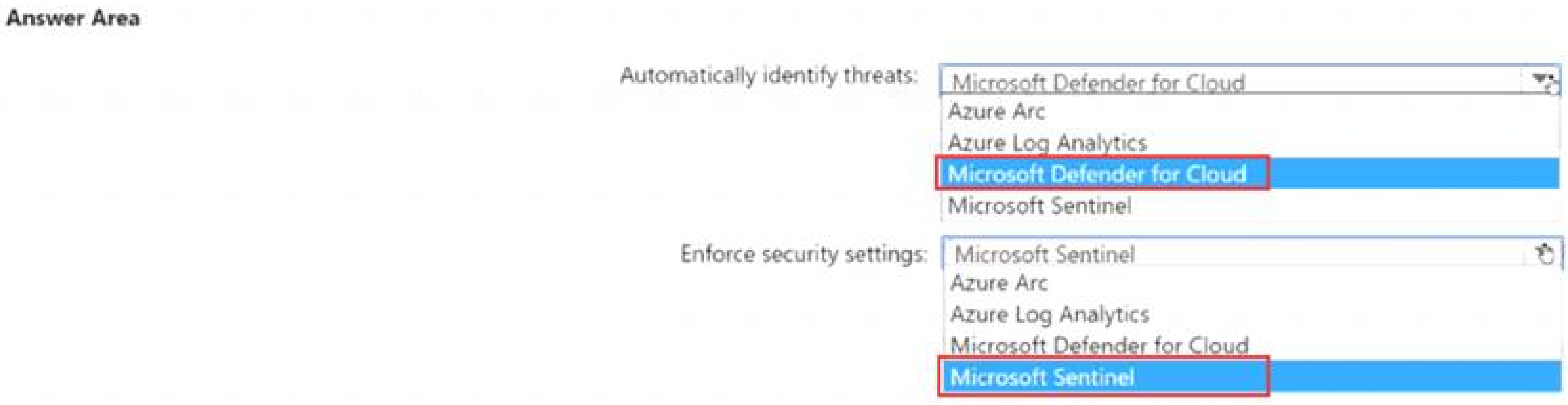
Automatically identify threats: Microsoft Defender for Cloud
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Enforce security settings: Microsoft Sentinel
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Automatically identify threats: Microsoft Defender for Cloud
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Enforce security settings: Microsoft Sentinel
- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

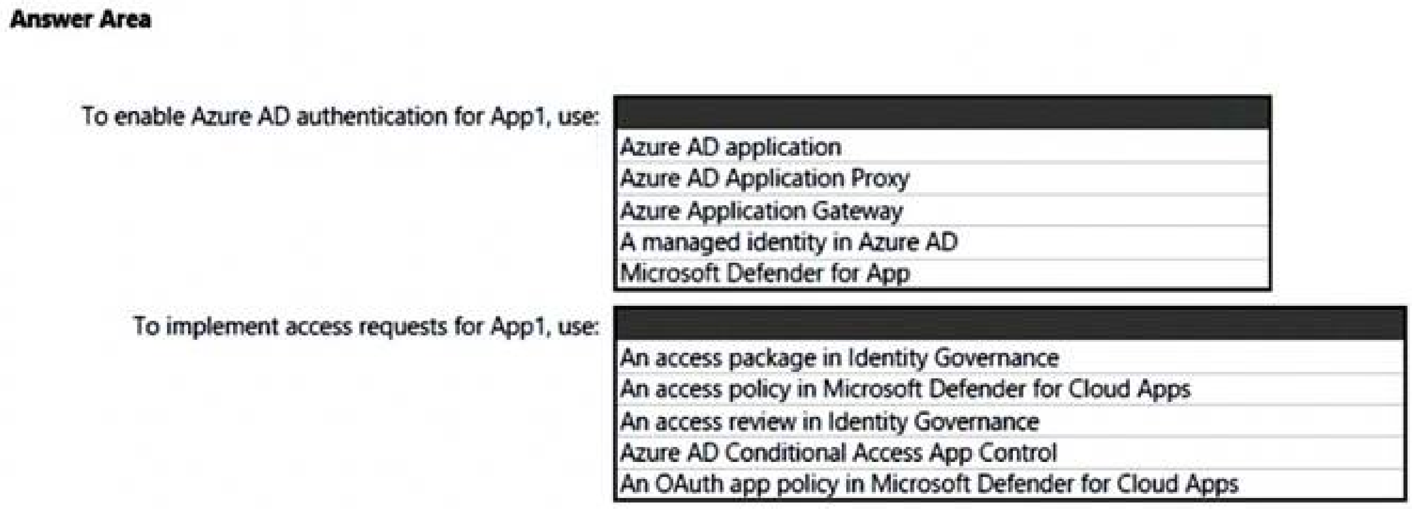
NEW QUESTION 56
- (Exam Topic 3)
You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

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 60
- (Exam Topic 3)
You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:
• Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
• Users will authenticate by using Azure Active Directory (Azure AD) user accounts. You need to recommend an access security architecture for App1.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

To enable Azure AD authentication for App1, use:
- Azure AD application
- Azure AD Application Proxy
- Azure Application Gateway
- A managed identity in Azure AD
- Microsoft Defender for App

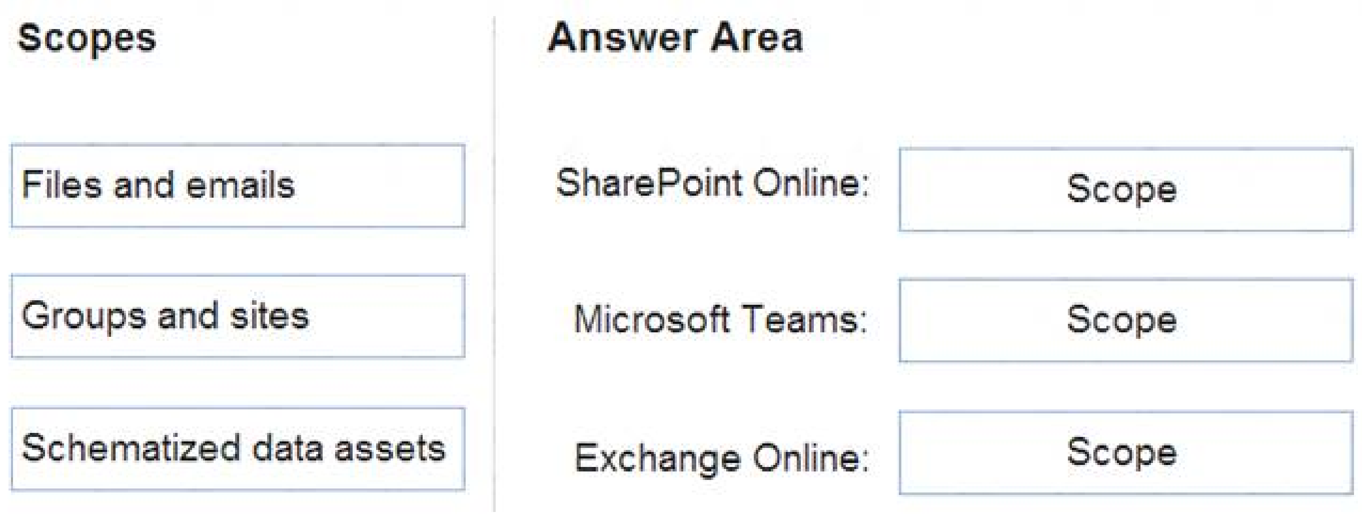
To implement access requests for App1, use:
- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- An access review in Identity Governance
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 65
- (Exam Topic 3)
Your company has Microsoft 365 E5 licenses and Azure subscriptions.
The company plans to automatically label sensitive data stored in the following locations:
• Microsoft SharePoint Online
• Microsoft Exchange Online
• Microsoft Teams
You need to recommend a strategy to identify and protect sensitive data.
Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Scopes

- Files and emails
- Groups and sites
- Schematized data assets

Answer Area

SharePoint Online: Scope

Microsoft Teams: Scope

Exchange Online: Scope

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails –
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide Go to label scopes

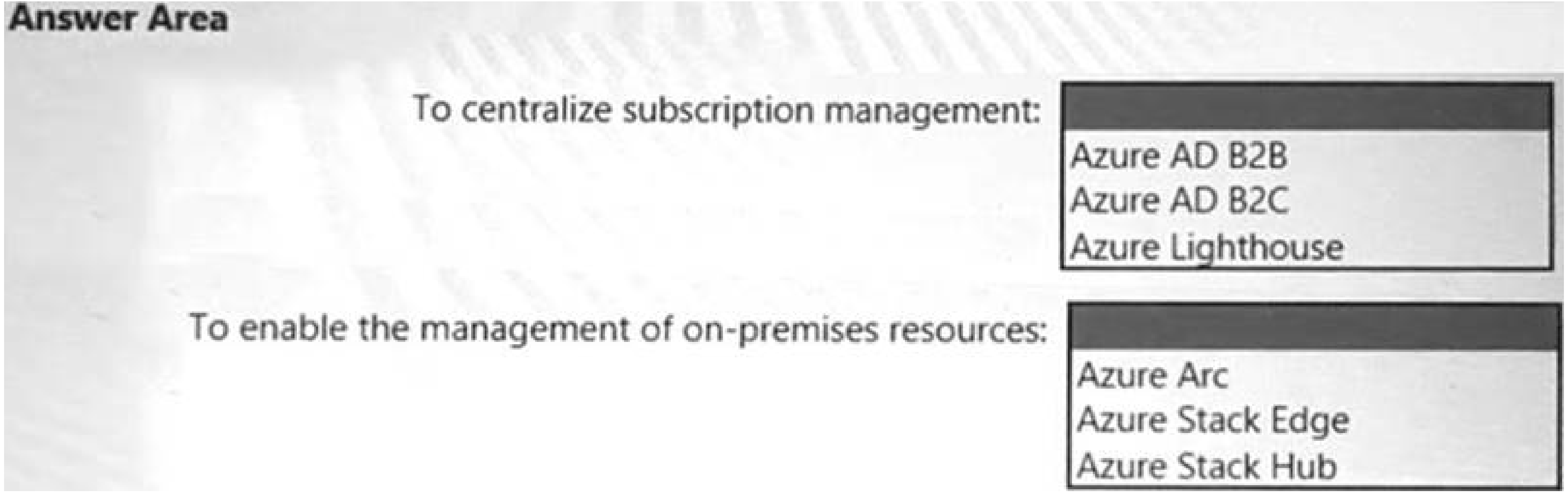
NEW QUESTION 69
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

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

Answer: C

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

NEW QUESTION 72
- (Exam Topic 2)
You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

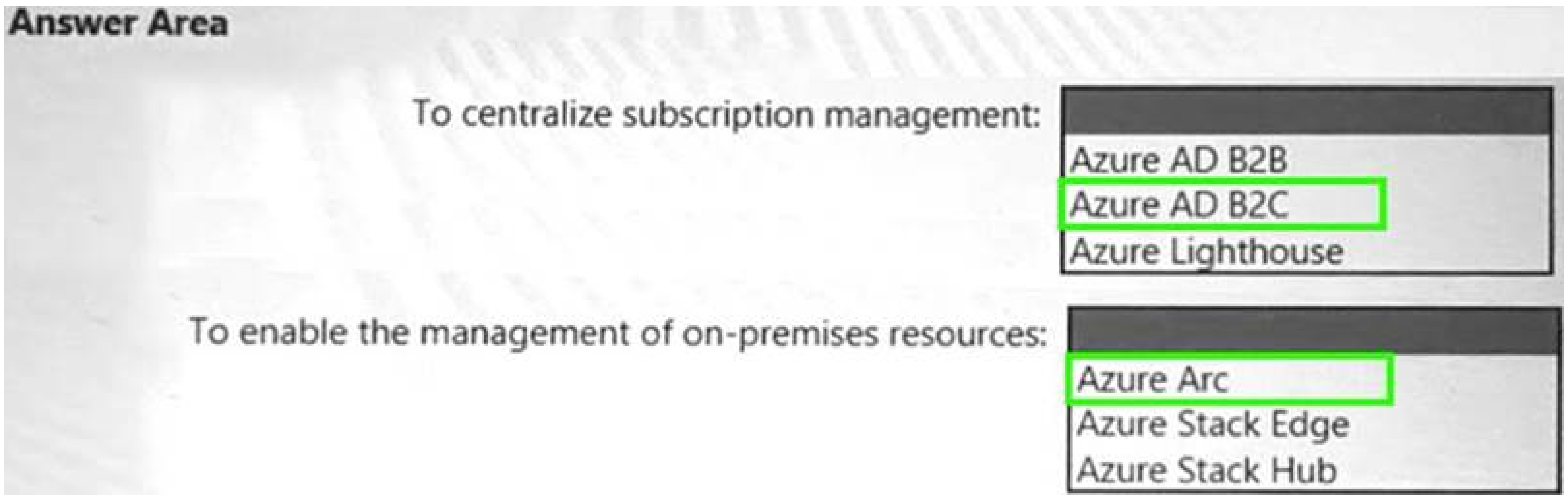
To centralize subscription management:
- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:
- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

To centralize subscription management:

- Azure AD B2B
- [✓ Azure AD B2C]
- Azure Lighthouse

To enable the management of on-premises resources:

- [✓ Azure Arc]
- Azure Stack Edge
- Azure Stack Hub

NEW QUESTION 75
- (Exam Topic 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

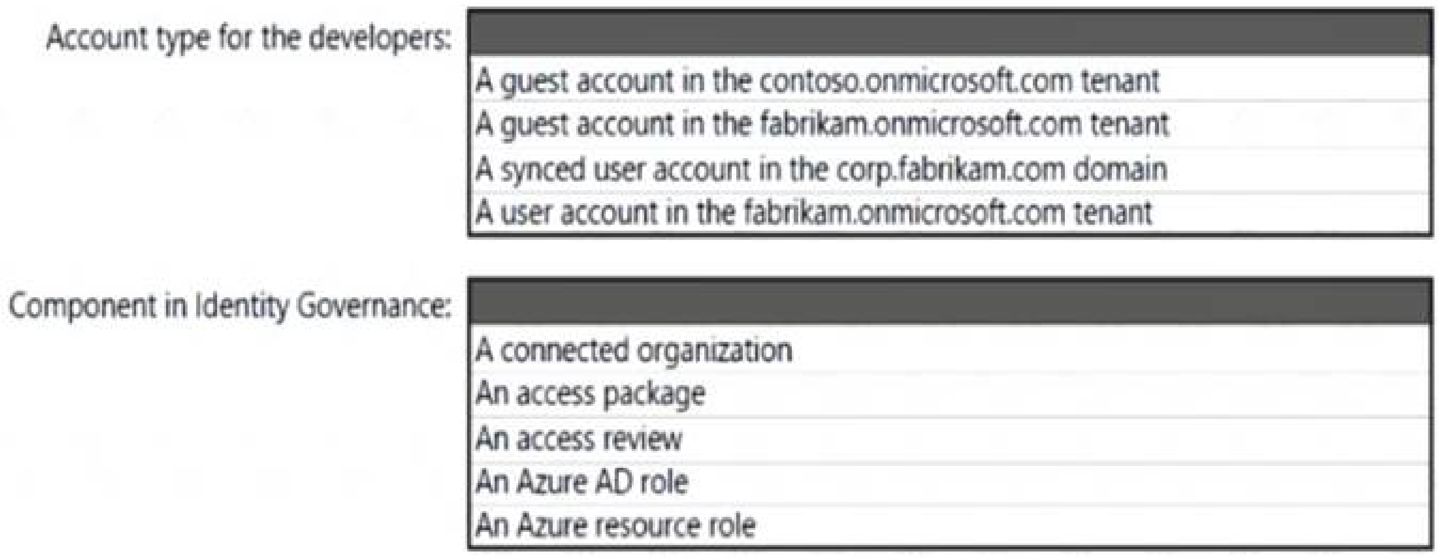
NEW QUESTION 76
- (Exam Topic 2)
You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.
What should you configure for each landing zone?

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

Answer: D

Explanation:
One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive. Given the landing zone requirements of
1) "Use a DNS namespace of litware.com"
2) "Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints"

NEW QUESTION 81
- (Exam Topic 1)
What should you create in Azure AD to meet the Contoso developer requirements?



Account type for the developers:

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

Component in Identity Governance:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A synced user account - Need to use a synched user account.
Box 2: An access review
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

NEW QUESTION 85
- (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 90
- (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 94
- (Exam Topic 3)
You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (O/CD) workflows for the deployment of applications to Azure. You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure. What should you recommend?

A. unit testing
B. penetration testing
C. dependency testing
D. threat modeling

Answer: C

NEW QUESTION 99
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 100
- (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

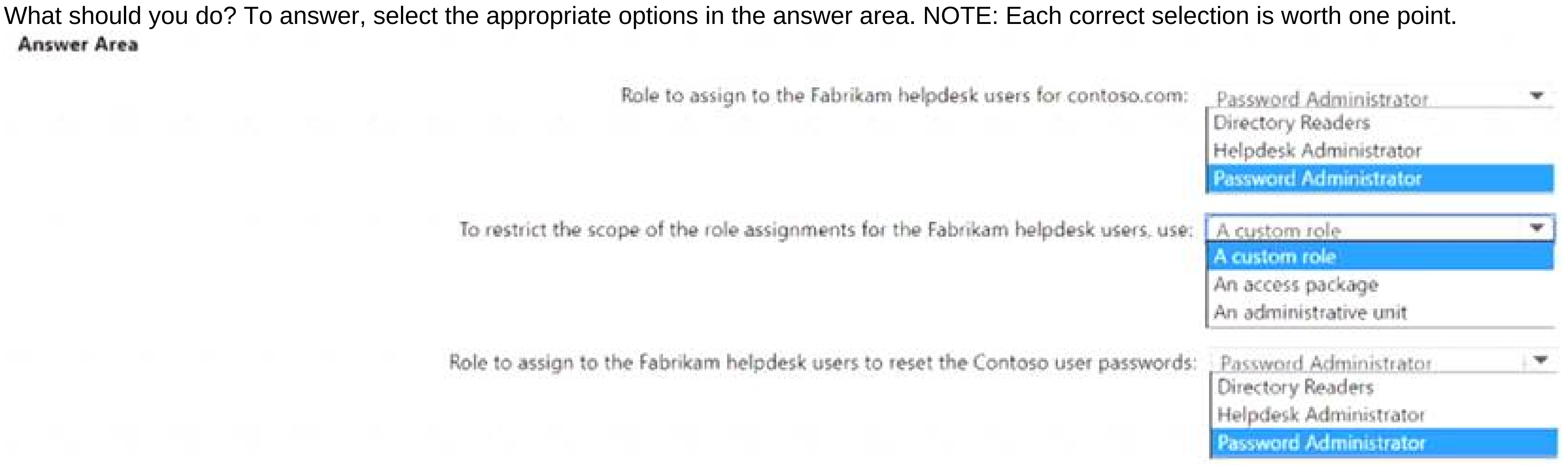
NEW QUESTION 104
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob 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 106
- (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.



Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com: Password Administrator
Directory Readers
Helpdesk Administrator
Password Administrator

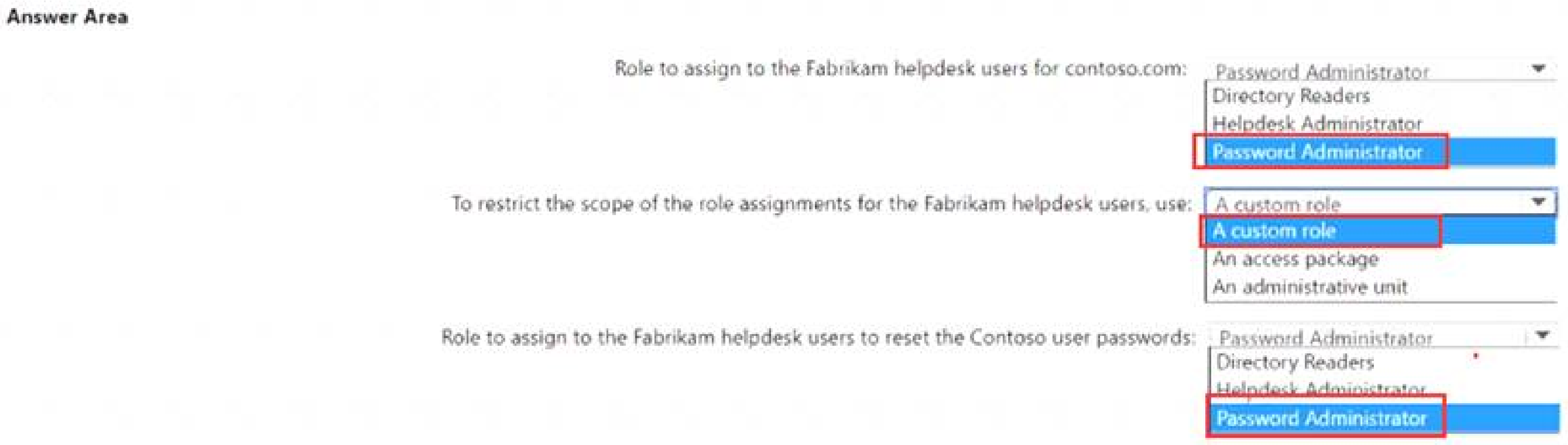
To restrict the scope of the role assignments for the Fabrikam helpdesk users, use: A custom role
A custom role
An access package
An administrative unit

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords: Password Administrator
Directory Readers
Helpdesk Administrator
Password Administrator

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com: Password Administrator
Directory Readers
Helpdesk Administrator
Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use: A custom role
A custom role
An access package
An administrative unit

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords: Password Administrator
Directory Readers
Helpdesk Administrator
Password Administrator

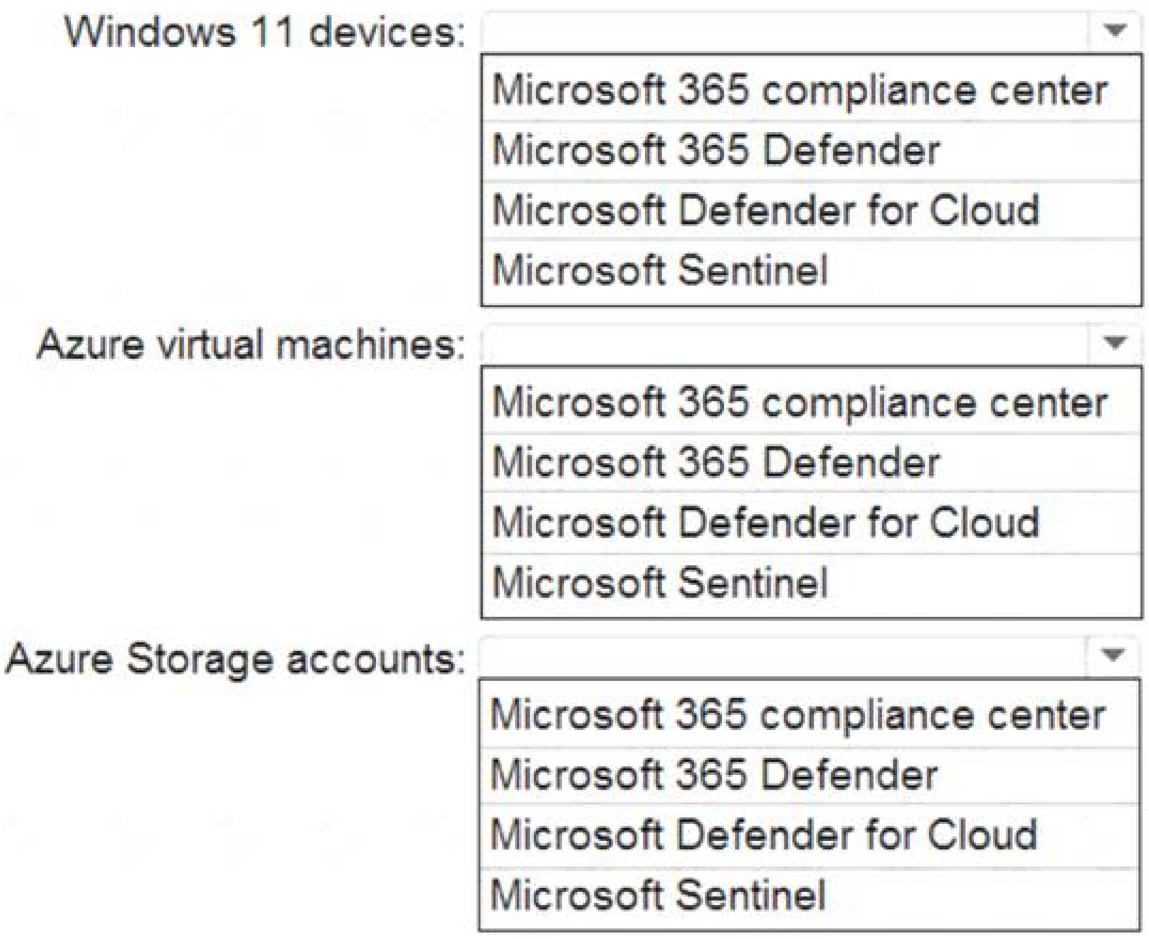
NEW QUESTION 109
- (Exam Topic 3)
You design cloud-based software as a service (SaaS) solutions.
You need to recommend ransomware attacks. The solution must follow Microsoft Security Best Practices. What should you recommend doing first?

A. Implement data protection.

B. Develop a privileged access strategy.
C. Prepare a recovery plan.
D. Develop a privileged identity strategy.

Answer: C

NEW QUESTION 112
- (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.



Windows 11 devices:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure virtual machines:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure Storage accounts:
- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

A. Mastered
B. Not Mastered

Answer: A

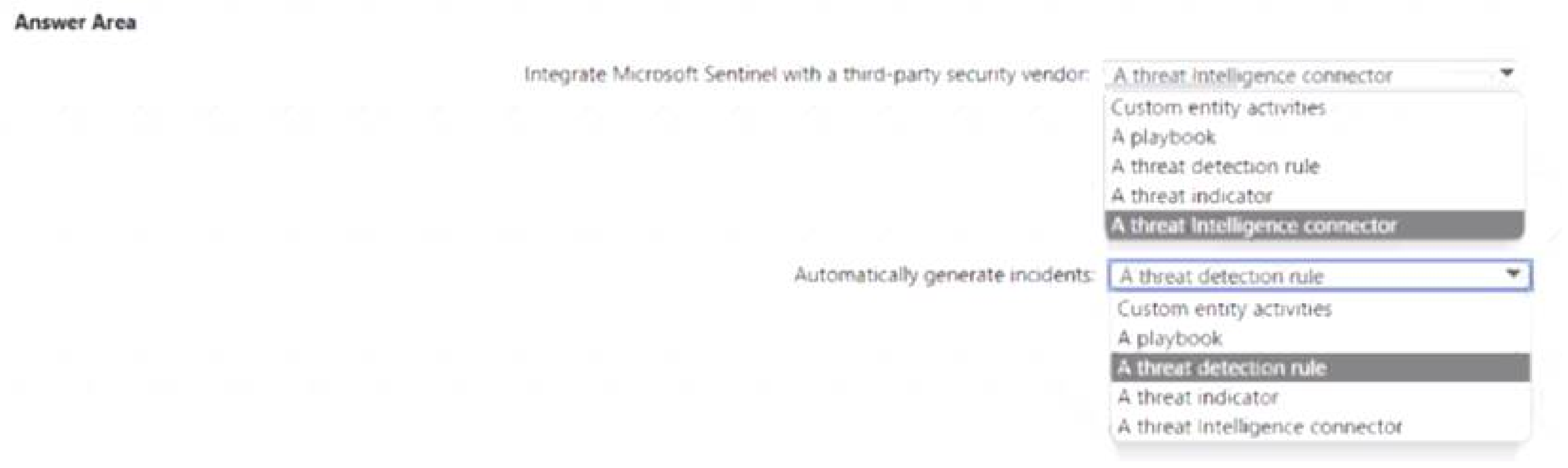
Explanation:
Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it). Selection 2: Microsoft Defender for Cloud.
Selection 3: Microsoft Defender for Cloud.
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-sec

NEW QUESTION 116
- (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 121
- (Exam Topic 3)
You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender
You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender
You need to recommend a solution to meet the following requirements:
• Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
• Automatically generate incidents when the IP address of a command-and control server is detected in the events
What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Integrate Microsoft Sentinel with a third-party security vendor: A threat intelligence connector

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat intelligence connector

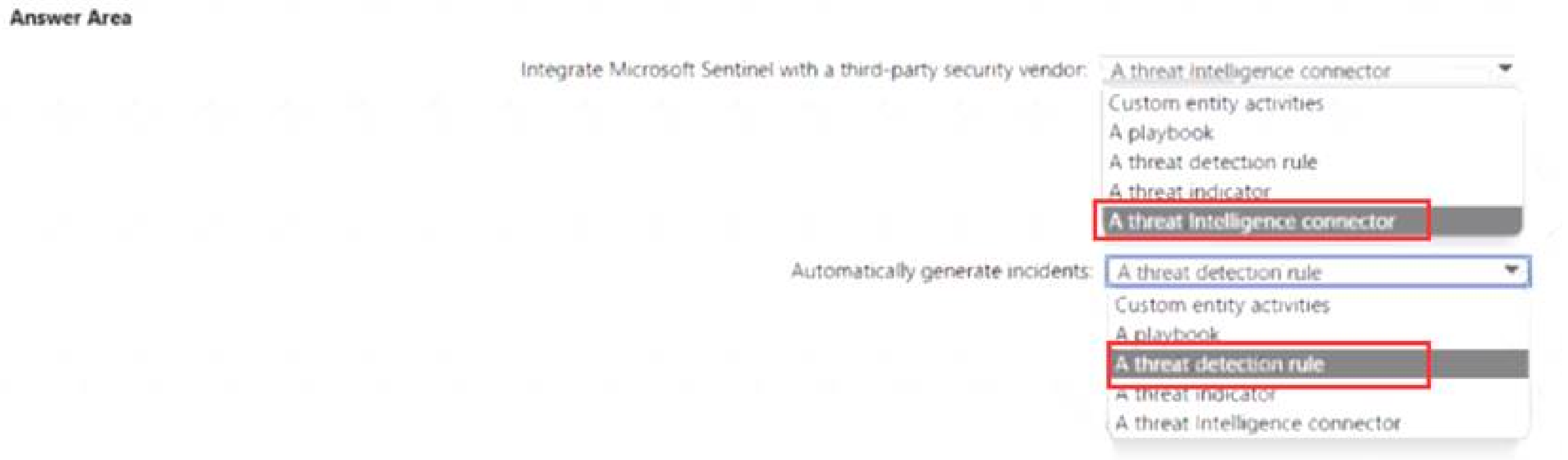
Automatically generate incidents: A threat detection rule

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat intelligence connector

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

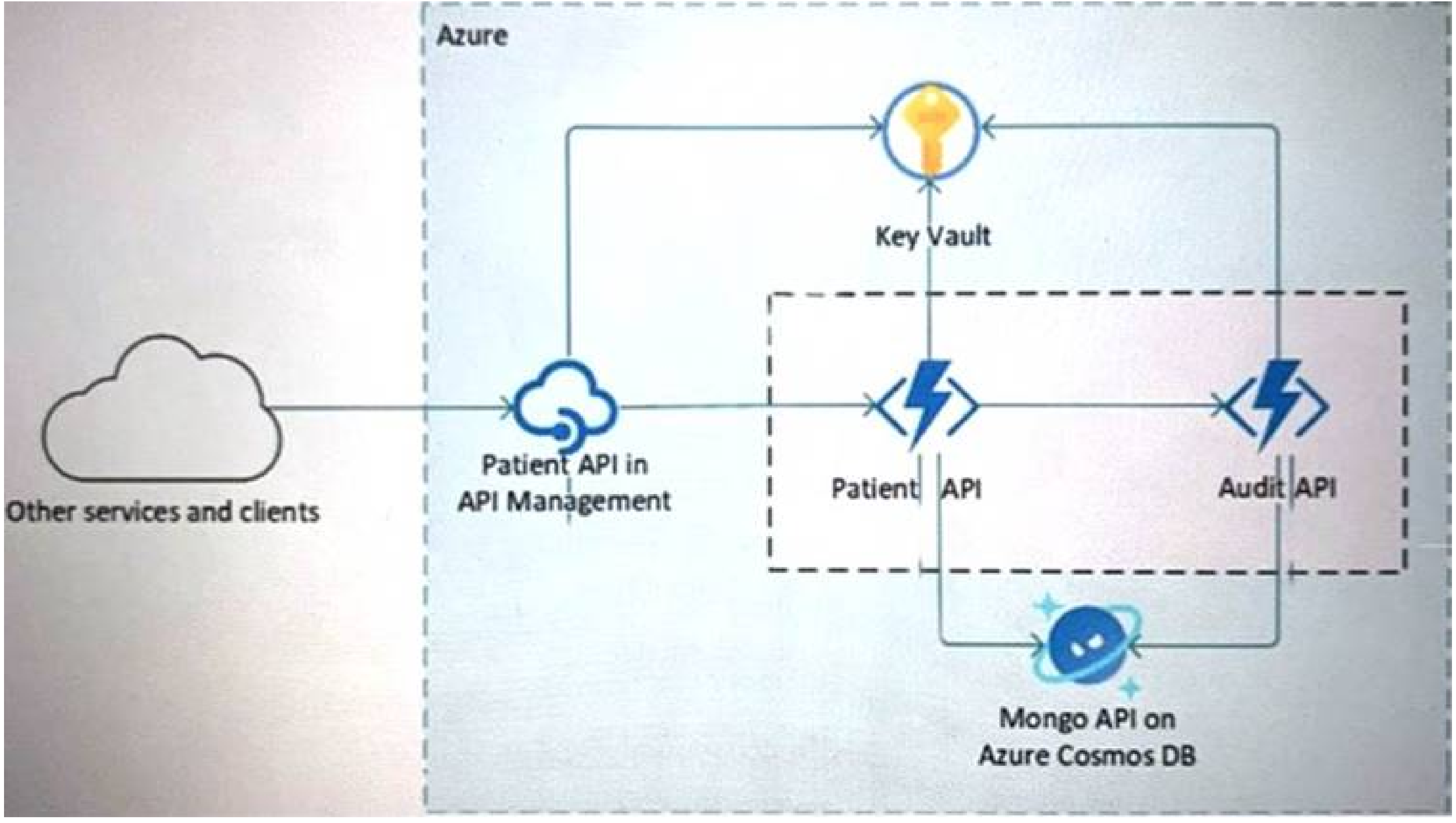
Integrate Microsoft Sentinel with a third-party security vendor: A threat intelligence connector

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat intelligence connector

Automatically generate incidents: A threat detection rule

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat intelligence connector

NEW QUESTION 125
- (Exam Topic 3)
Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.


Azure
Key Vault
Other services and clients
Patient API in API Management
Patient API
Audit API
Mongo API on Azure Cosmos DB

You need to recommend a solution to isolate the compute components on an Azure virtual network. What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications
B. an Azure App Service Environment (ASE)
C. Azure service endpoints
D. an Azure Active Directory (Azure AD) application proxy

Answer: B

Explanation:
App Service environments (ASEs) are appropriate for application workloads that require:
Very high scale,Isolation and secure network access,High memory utilization.This capability can host your: Windows web apps,Linux web apps

Docker containers,Mobile apps Functions
https://docs.microsoft.com/en-us/azure/app-service/environment/overview

NEW QUESTION 130
- (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 137
- (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 140
- (Exam Topic 3)
You have an Azure AD tenant that syncs with an Active Directory Domain Services {AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.
You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.
You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows
computers only when access is required. The solution must minimize the lateral movement of ransomware
attacks if an administrator account on a computer is compromised.
What should you include in the recommendation?

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

Answer: A

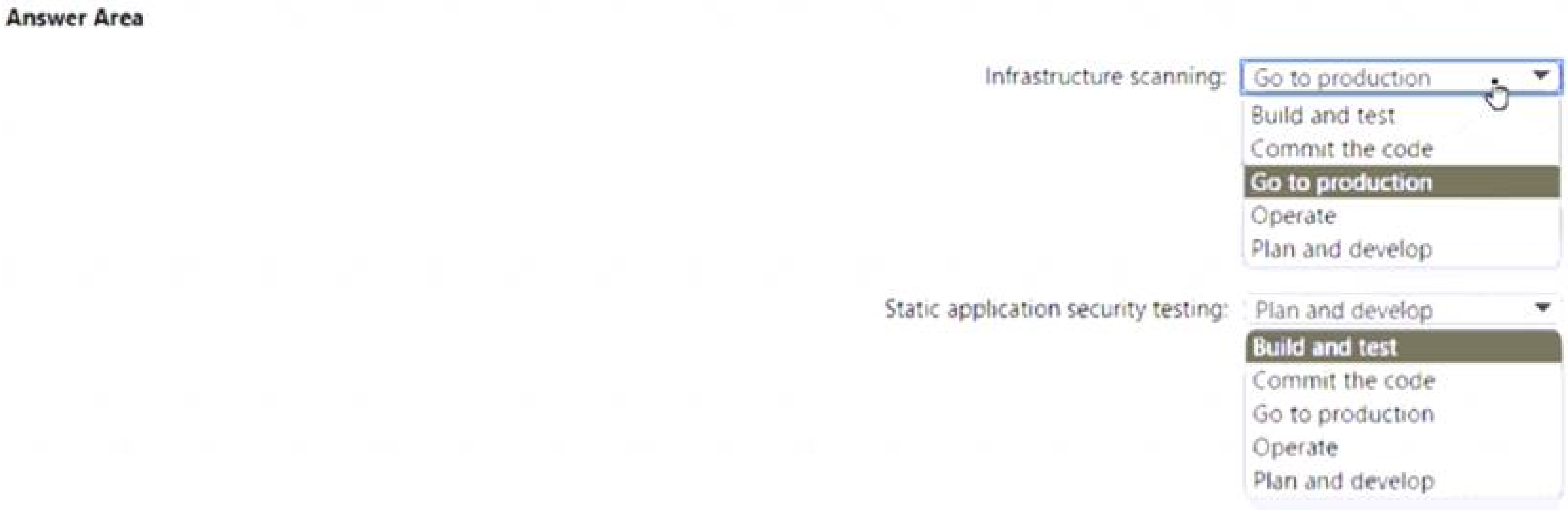
NEW QUESTION 142
- (Exam Topic 3)
Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities. You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

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

Answer: B

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

NEW QUESTION 145
- (Exam Topic 3)
Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines
You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines. What should recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

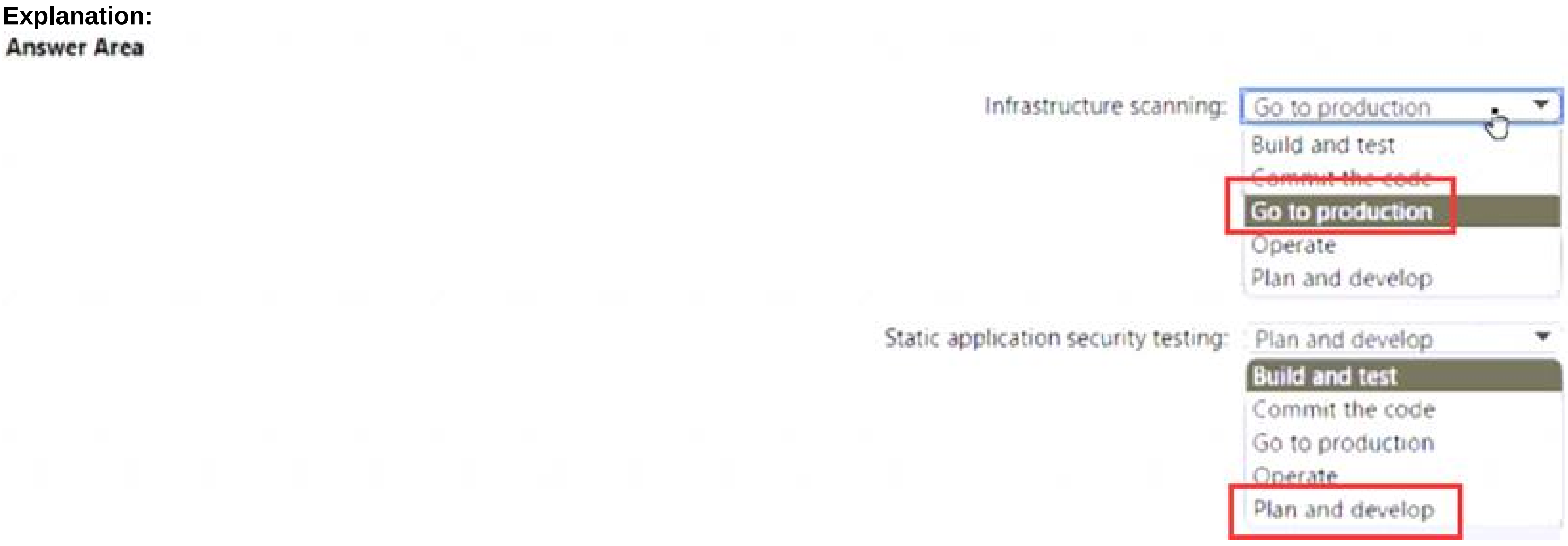
Infrastructure scanning: Go to production

Static application security testing: Plan and develop

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Infrastructure scanning: Go to production

Static application security testing: Plan and develop

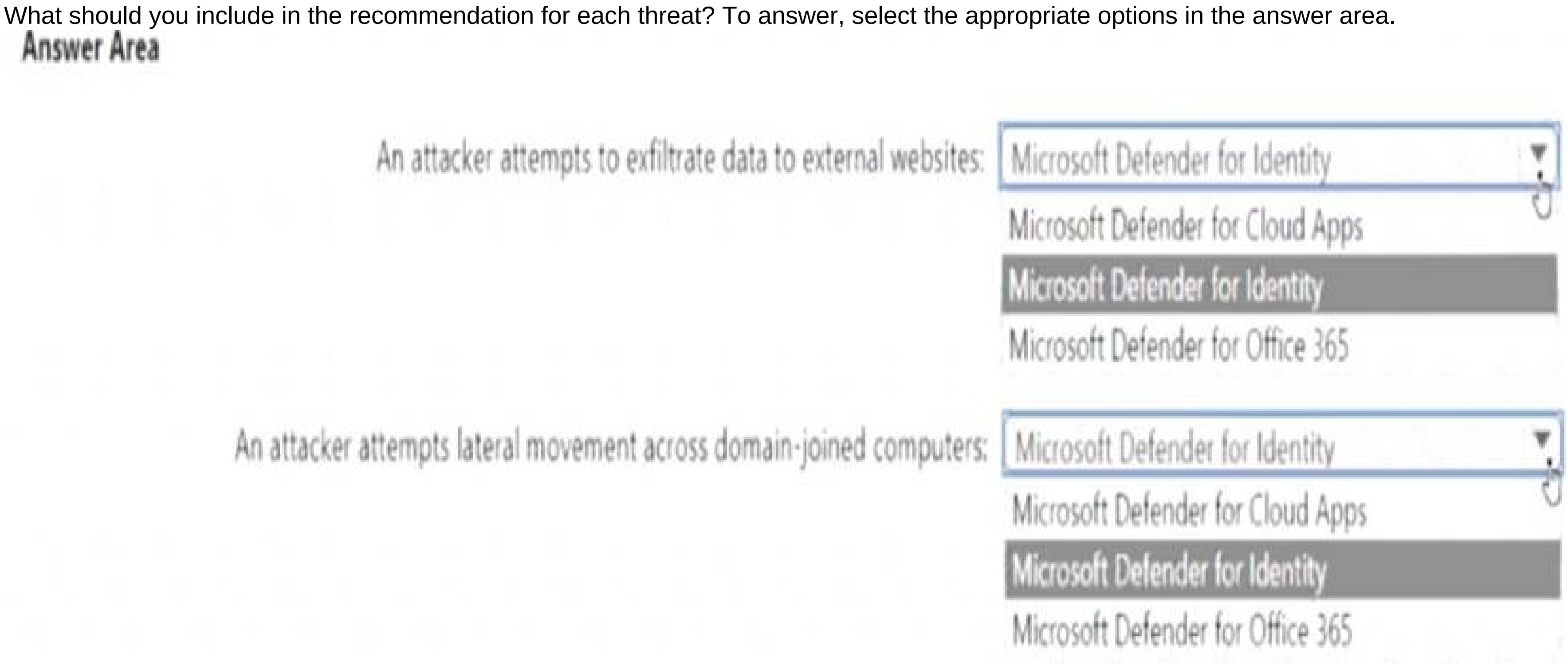
NEW QUESTION 149
- (Exam Topic 3)
Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app.
You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection. What should you include in the recommendation?

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

Answer: D

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

NEW QUESTION 150
- (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.



Answer Area

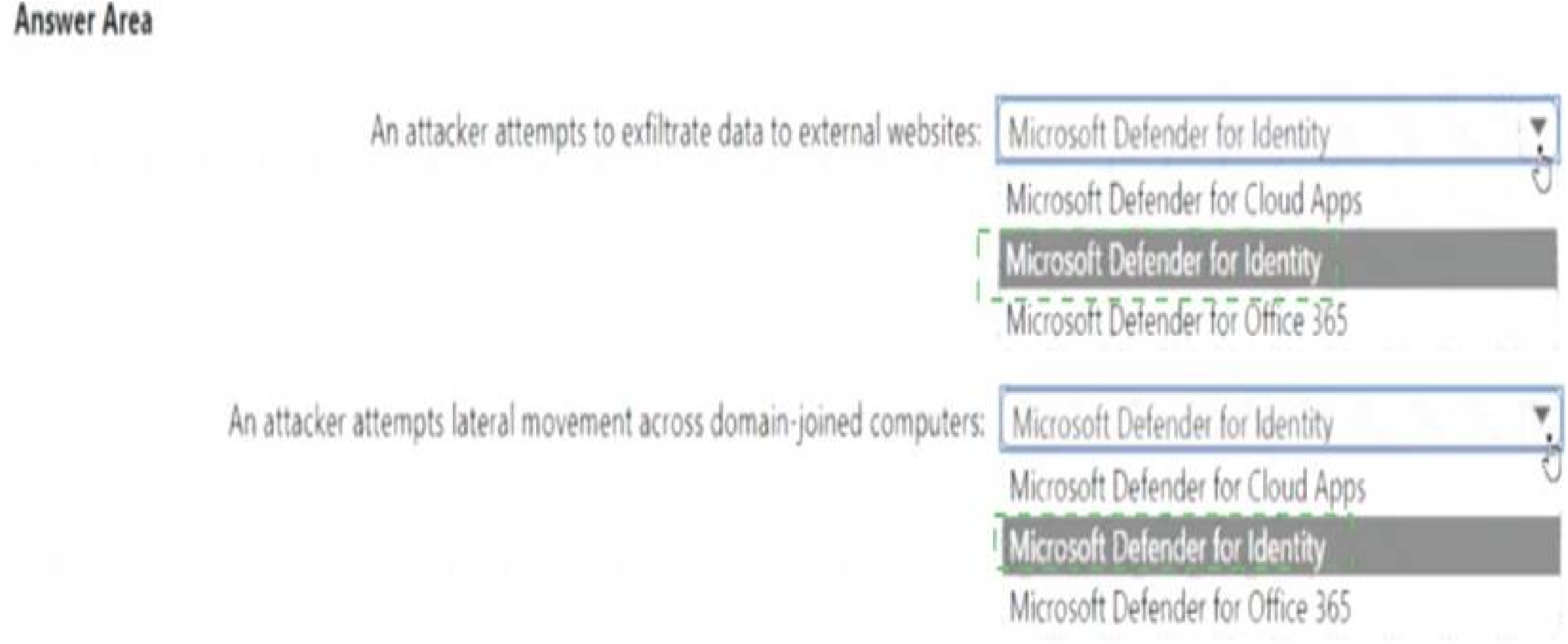
An attacker attempts to exfiltrate data to external websites: Microsoft Defender for Identity ▼
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers: Microsoft Defender for Identity ▼
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

A. Mastered
B. Not Mastered

Answer: A

Explanation:

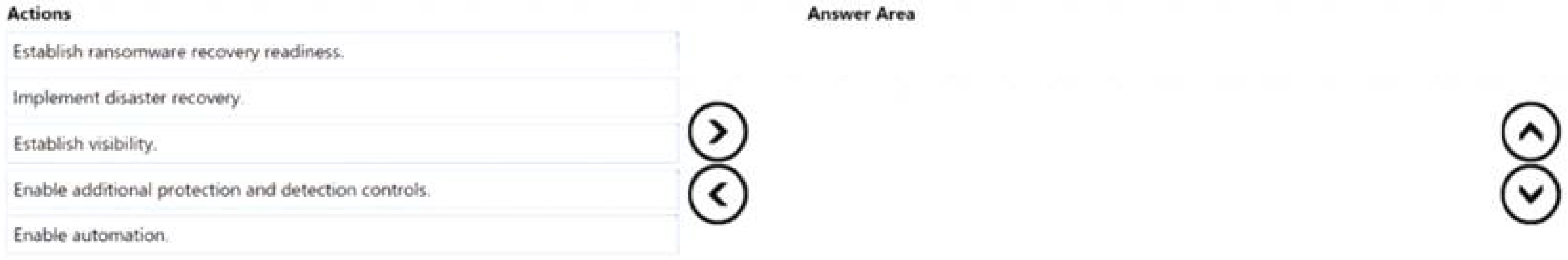


Answer Area

An attacker attempts to exfiltrate data to external websites: Microsoft Defender for Identity ▼
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers: Microsoft Defender for Identity ▼
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Office 365

NEW QUESTION 152
- (Exam Topic 3)
You are designing a security operations strategy based on the Zero Trust framework.
You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).
Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer, move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.



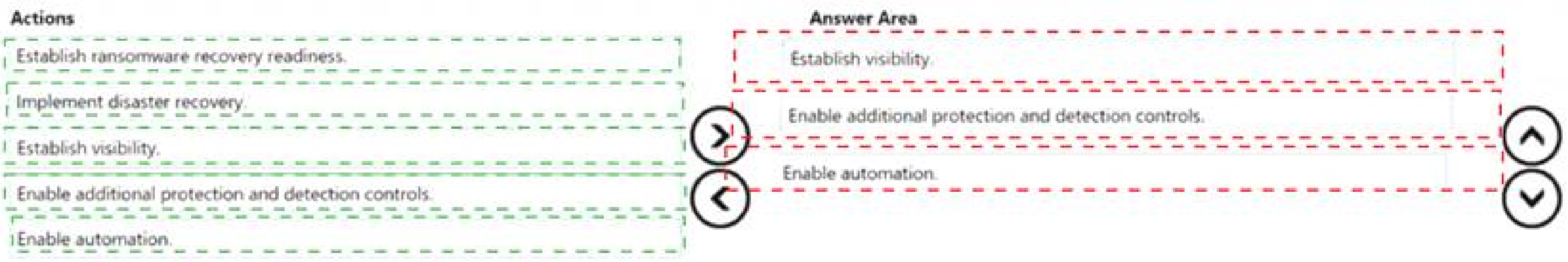
Actions
Establish ransomware recovery readiness.
Implement disaster recovery.
Establish visibility.
Enable additional protection and detection controls.
Enable automation.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

- Establish ransomware recovery readiness.
- Implement disaster recovery.
- Establish visibility.
- Enable additional protection and detection controls.
- Enable automation.

Answer Area

- Establish visibility.
- Enable additional protection and detection controls.
- Enable automation.

NEW QUESTION 156

- (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

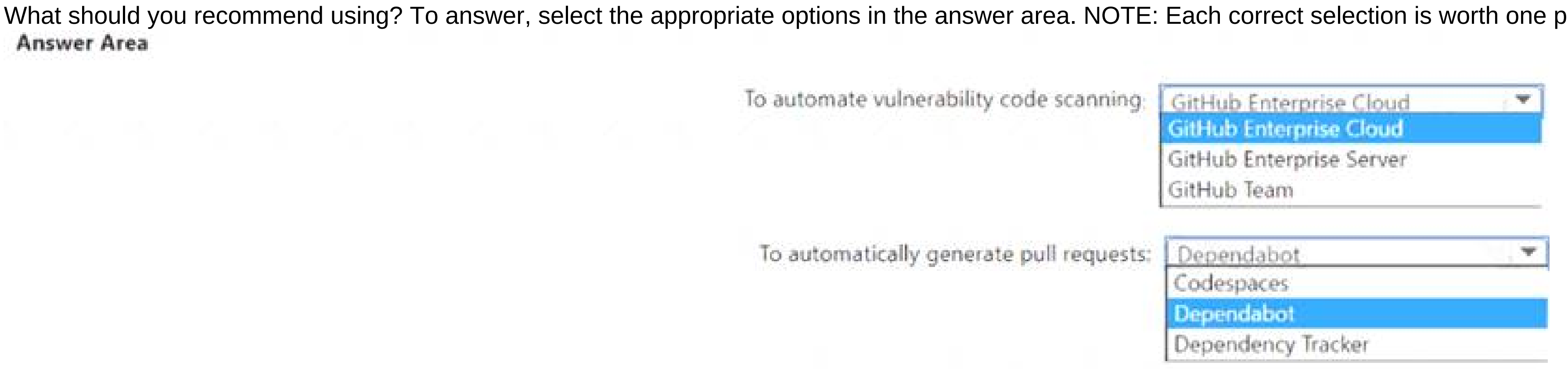
NEW QUESTION 160

- (Exam Topic 3)

You plan to automate the development and deployment of a Nodejs-based app by using GitHub. You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

- Automate the generation of pull requests that remediate identified vulnerabilities.
- Automate vulnerability code scanning for public and private repositories.
- Minimize administrative effort.
- Minimize costs.

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



Answer Area

To automate vulnerability code scanning: GitHub Enterprise Cloud

- GitHub Enterprise Cloud
- GitHub Enterprise Server
- GitHub Team

To automatically generate pull requests: Dependabot

- Codespaces
- Dependabot
- Dependency Tracker

A. Mastered
B. Not Mastered

Answer: A

Explanation:

A close up of a text Description automatically generated

NEW QUESTION 163

- (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

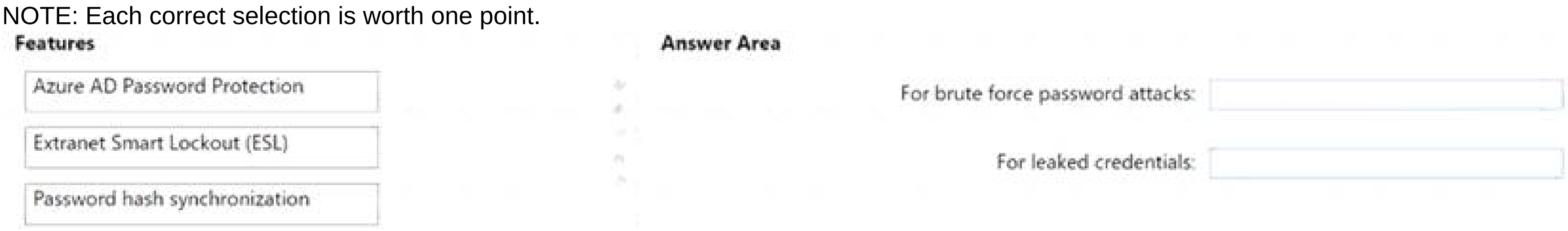
Answer: C

NEW QUESTION 168

- (Exam Topic 3)

You have a hybrid Azure AD tenant that has pass-through authentication enabled. You are designing an identity security strategy.

You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.
What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Features

Azure AD Password Protection

Extranet Smart Lockout (ESL)

Password hash synchronization

Answer Area

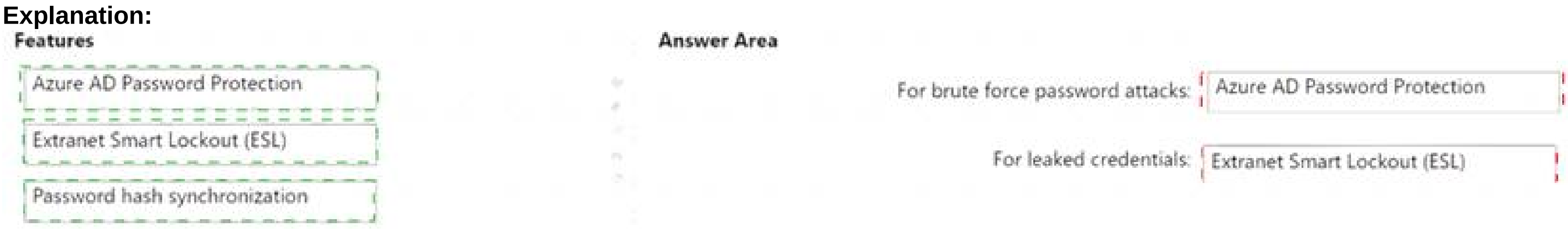
For brute force password attacks:

For leaked credentials:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Features

Azure AD Password Protection

Extranet Smart Lockout (ESL)

Password hash synchronization

Answer Area

For brute force password attacks: Azure AD Password Protection

For leaked credentials: Extranet Smart Lockout (ESL)

NEW QUESTION 170
- (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 174
......