



## **Microsoft**

### **Exam Questions SC-100**

Microsoft Cybersecurity Architect

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling the VMAccess extension on all virtual machines.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s> Adaptive Network Hardening:  
<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

### NEW QUESTION 2

- (Exam Topic 3)

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 adaptive network hardening.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

#### Explanation:

JIT:  
<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s>  
Adaptive Network Hardening:  
<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

### NEW QUESTION 3

- (Exam Topic 3)

You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:

- Encrypt cardholder data by using encryption keys managed by the company.
- Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
- B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
- C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
- D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

**Answer:** AC

#### Explanation:

<https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service-encryption/>

### NEW QUESTION 4

- (Exam Topic 3)

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

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

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

**Answer:** ABD

### NEW QUESTION 5

- (Exam Topic 3)

You have an operational model based on the Microsoft Cloud Adoption framework for Azure.

You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, database, files, and storage accounts.

What should you include in the recommendation?

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

**Answer:** A

**NEW QUESTION 6**

- (Exam Topic 3)

Your company wants to optimize ransomware incident investigations.

You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.

Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
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:**

Actions	Answer Area
Implement a comprehensive strategy to reduce the risk of privileged access compromise.	1 Assess the current situation and identify the scope.
Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.	2 Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.
	3 Identify the compromise recovery process.

**NEW QUESTION 7**

- (Exam Topic 3)

You have a 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 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**

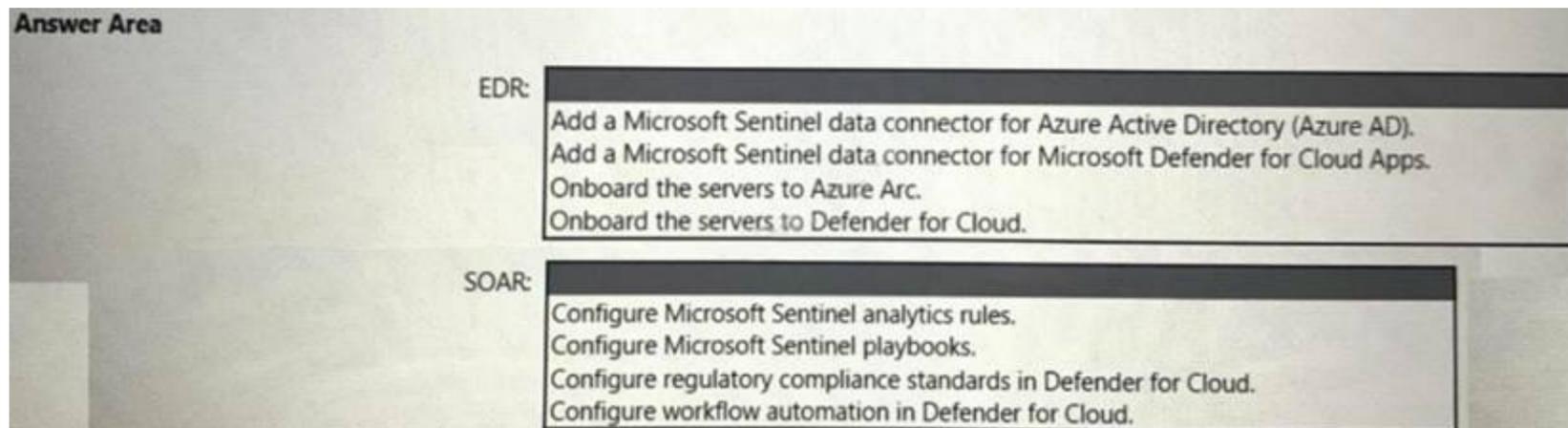
- (Exam Topic 3)

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure. You plan to deploy Azure virtual machines that will run Windows Server. You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

For SOAR read this <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks> Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of Microsoft Defender.

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide>

**NEW QUESTION 10**

- (Exam Topic 3)

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)

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 15**

- (Exam Topic 3)

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

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

**Answer:** AB

**Explanation:**

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

**NEW QUESTION 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 AD credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. a relying party trust in Active Directory Federation Services (AD FS)
- C. Azure AD Application Proxy
- D. Azure AD B2C

**Answer:** A

**NEW QUESTION 23**

- (Exam Topic 3)

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 24**

- (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 25**

- (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



**NEW QUESTION 30**

- (Exam Topic 3)

You are designing a ransomware response plan that follows Microsoft Security Best Practices

You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out.

What should you include in the recommendations?

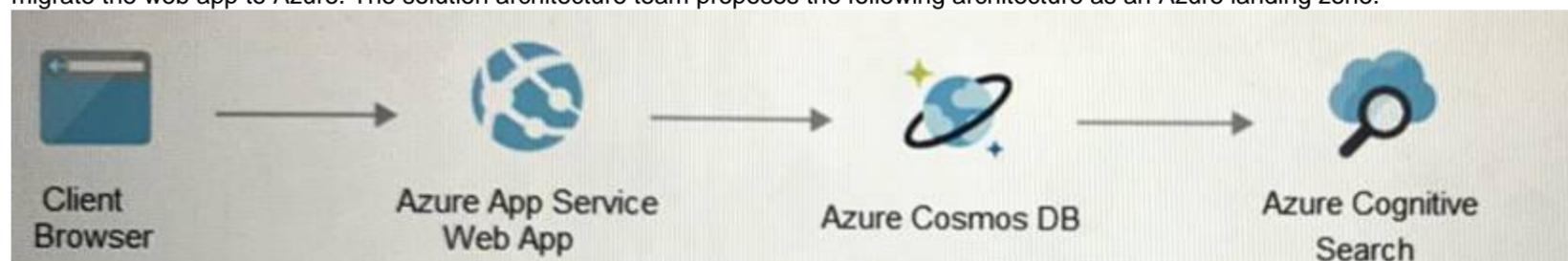
- A. Privileged Access Workstations (PAWs)
- B. emergency access accounts
- C. device compliance policies
- D. Customer Lockbox for Microsoft Azure

**Answer: B**

**NEW QUESTION 35**

- (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 38**

- (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 43**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.

You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.

Which two components should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. data loss prevention (DLP) policies

- B. sensitivity label policies
- C. retention label policies
- D. eDiscovery cases

**Answer:** AB

**Explanation:**

Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate. Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used alongside capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.

<https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/> <https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?vie>

**NEW QUESTION 46**

- (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 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 53**

- (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 in near-real-time (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 56**

- (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:

Microsoft Teams:

Exchange Online:

- 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 61**

- (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 66**

- (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 70**

- (Exam Topic 2)

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Security Assertion Markup Language (SAML)
- B. NTLMv2
- C. certificate-based authentication
- D. Kerberos

**Answer:** AD

**Explanation:**

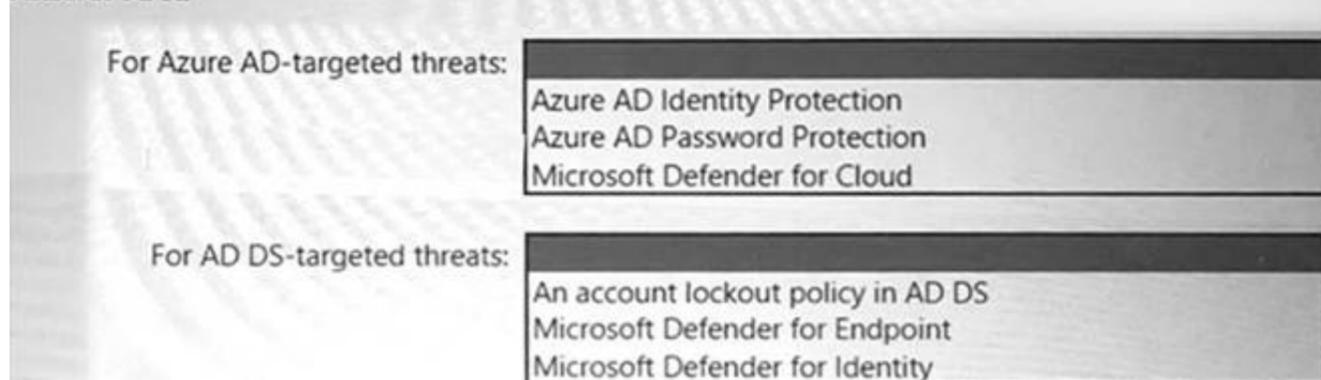
<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-o> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-w> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain>

**NEW QUESTION 74**

- (Exam Topic 2)

You need to 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.

**Answer Area**



The screenshot shows an 'Answer Area' with two sections for selecting security solutions:

- For Azure AD-targeted threats:**
  - Azure AD Identity Protection
  - Azure AD Password Protection
  - Microsoft Defender for Cloud
- For AD DS-targeted threats:**
  - An account lockout policy in AD DS
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Identity

- 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 78**

- (Exam Topic 2)

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

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

**Answer Area**

Evaluate regulatory compliance of cloud resources by assigning:

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

Evaluate regulatory compliance of on-premises resources by using:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Evaluate regulatory compliance of cloud resources by assigning:

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

Evaluate regulatory compliance of on-premises resources by using:

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

**NEW QUESTION 79**

- (Exam Topic 2)

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

**Answer Area**

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

- Private endpoints
- Service endpoints
- Virtual network integration

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

- Private endpoints
- Service endpoints
- Virtual network integration

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Virtual Network Integration - correct

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

Box 2: Private Endpoints. - correct

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

**NEW QUESTION 84**

- (Exam Topic 1)

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

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

**Answer Area**

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

- A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

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

while it is in policy assignment

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

**NEW QUESTION 89**

- (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 synced 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 91**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image."

<https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image>

**NEW QUESTION 93**

- (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 97**

- (Exam Topic 1)

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

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

**Answer Area**

ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

**NEW QUESTION 101**

- (Exam Topic 3)

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance. Solution: You recommend configuring gateway-required virtual network integration. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

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

**NEW QUESTION 102**

- (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 103**

- (Exam Topic 3)

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

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

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 108**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 112**

- (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

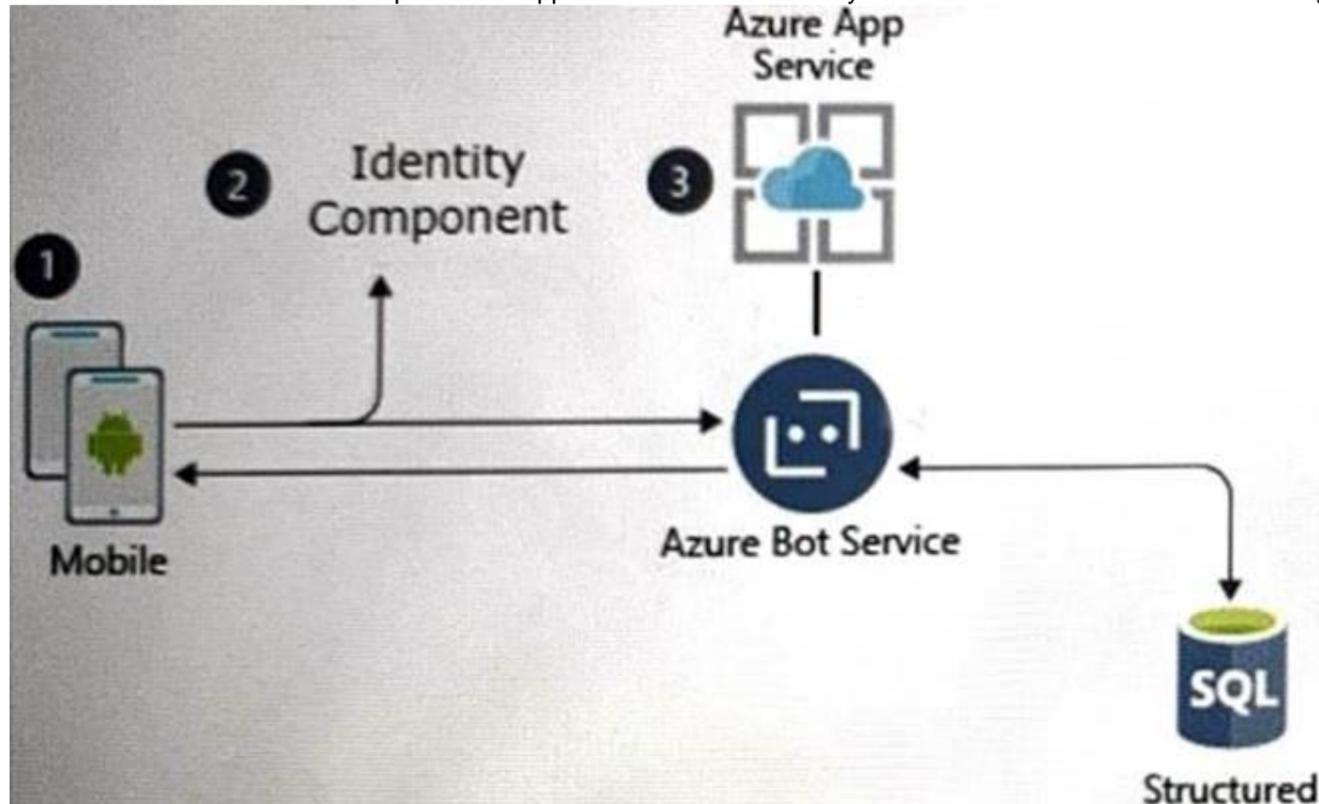
**Explanation:**

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

**NEW QUESTION 117**

- (Exam Topic 3)

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

- Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
- Be managed separately from the identity store of the customer.
- Support fully customizable branding for each app.

Which service should you recommend to complete the design?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 118**

- (Exam Topic 3)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 120**

- (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 125**

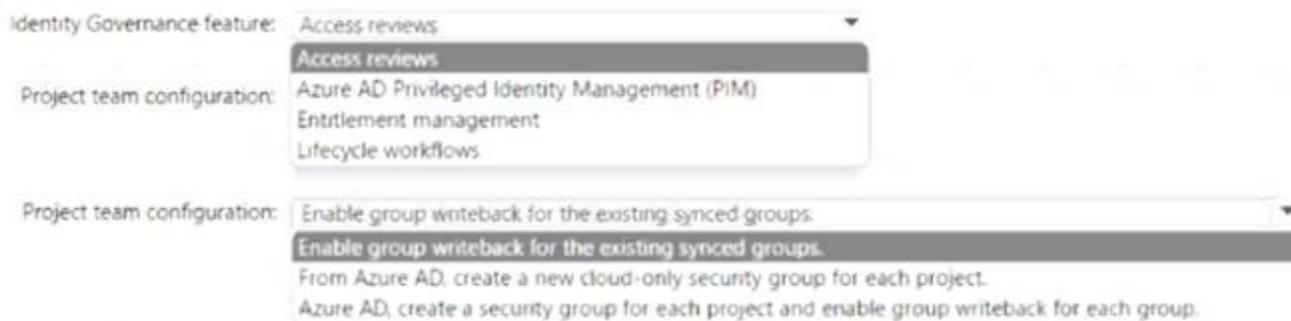
- (Exam Topic 3)

Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled. You have a Microsoft 365 subscription that uses Microsoft SharePoint Online. You have multiple project teams. Each team has an AD DS group that syncs with Azure AD. Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams. You need to recommend an Azure AD identity Governance solution that meets the following requirements:

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

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

**Answer Area**

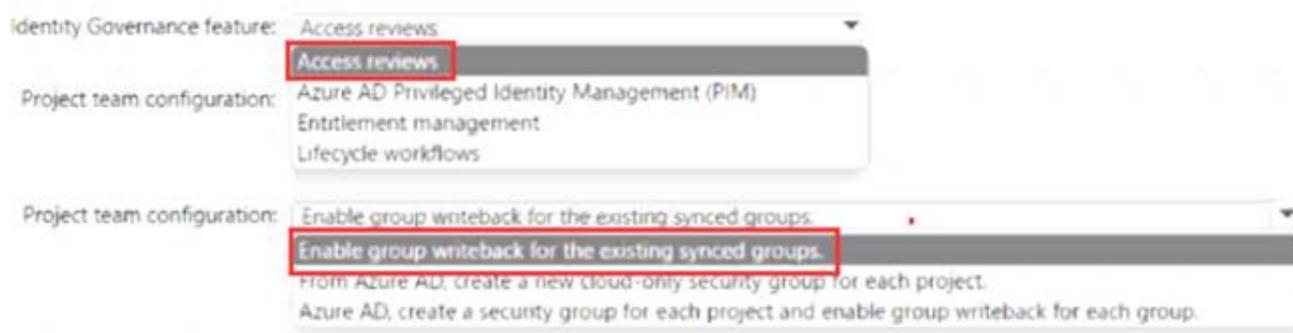


- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area



**NEW QUESTION 127**

- (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 129**

- (Exam Topic 3)

Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

- Minimizes manual intervention by security operation analysts
  - Supports Waging alerts within Microsoft Teams channels
- What should you include in the strategy?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 134**

- (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**

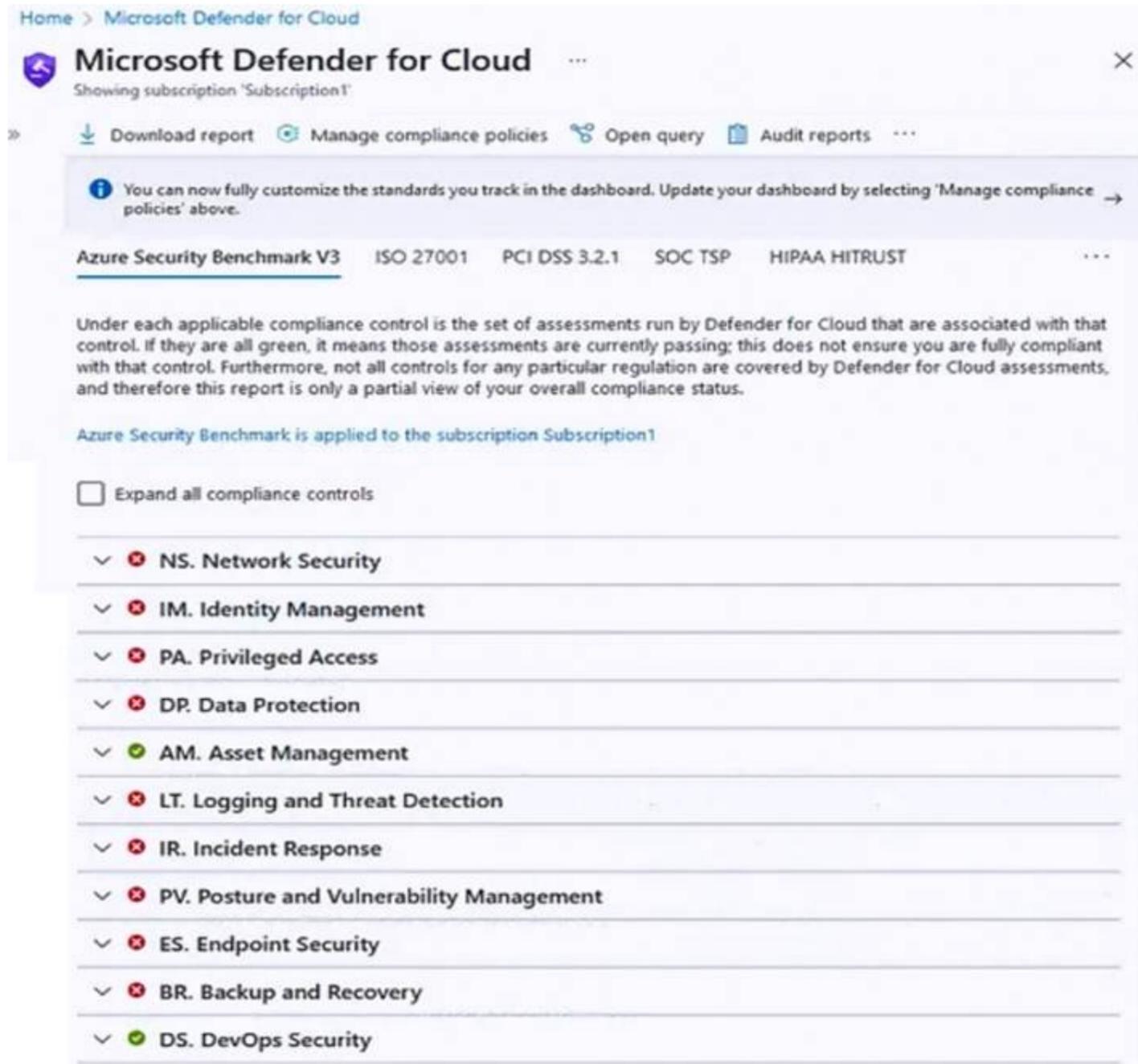
**Explanation:**

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

**NEW QUESTION 137**

- (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 139**

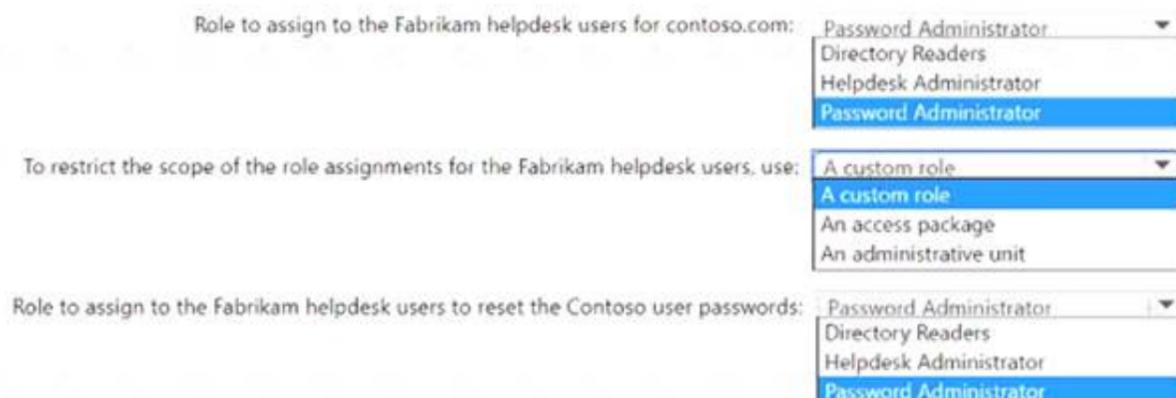
- (Exam Topic 3)

Your company, named Contoso. Ltd... has an Azure AD tenant named contoso.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**

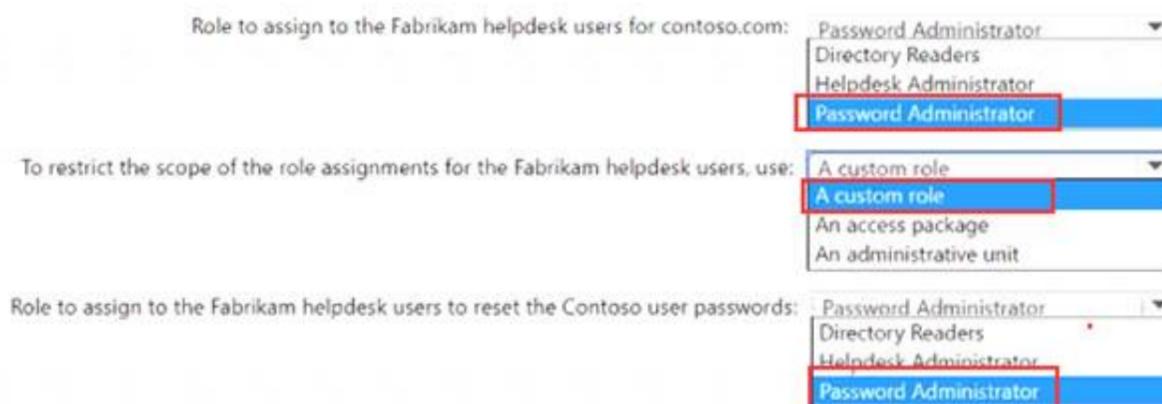


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area



**NEW QUESTION 143**

- (Exam Topic 3)

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

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

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

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

**Answer:** DE

**Explanation:**

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

**NEW QUESTION 145**

- (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 servers 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 149**

- (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 150**

- (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 151**

- (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.

**Answer Area**

Azure Backup: Encryption by using platform-managed keys  
 Access policies  
 Access tiers  
 Encryption by using platform-managed keys  
 Immutable storage  
 A security PIN

Azure Storage: Immutable storage  
 Access policies  
 Access tiers  
 Encryption by using platform-managed keys  
 Immutable storage  
 A security PIN

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Azure Backup: Encryption by using platform-managed keys  
 Access policies  
 Access tiers  
 Encryption by using platform-managed keys  
 Immutable storage  
 A security PIN

Azure Storage: Immutable storage  
 Access policies  
 Access tiers  
 Encryption by using platform-managed keys  
 Immutable storage  
 A security PIN

**NEW QUESTION 154**

- (Exam Topic 3)

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

Azure virtual machines:

Azure Storage accounts:

- 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 158**

- (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:

Automatically generate incidents:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area



**NEW QUESTION 162**

- (Exam Topic 3)

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

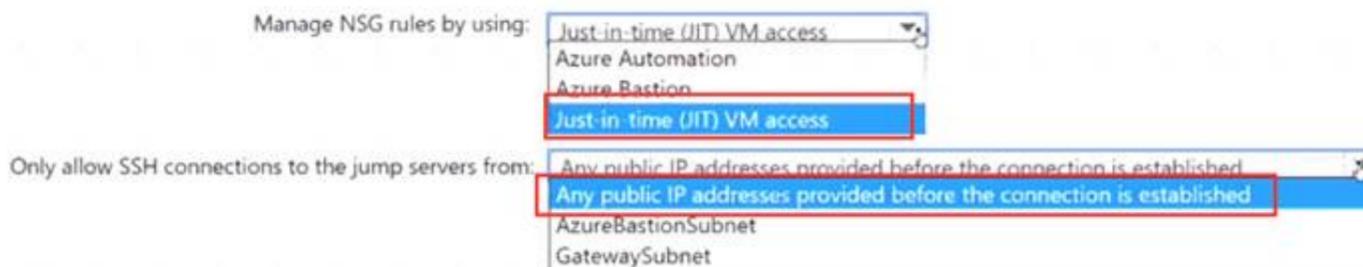


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

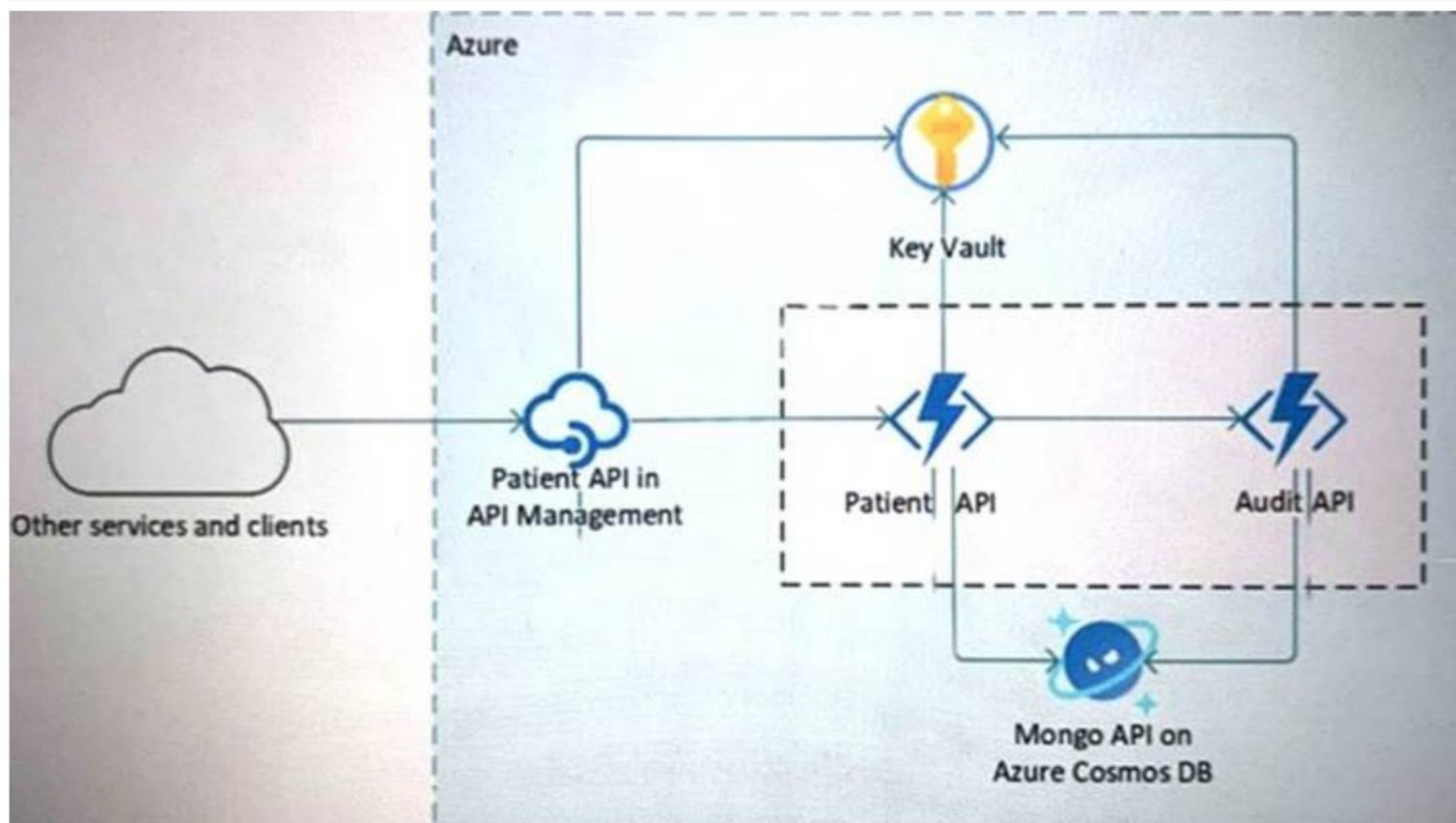
Answer Area



**NEW QUESTION 163**

- (Exam Topic 3)

Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.



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 164**

- (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 165**

- (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 170**

- (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 175**

- (Exam Topic 3)

You have an Active Directory Domain Services (AD DS) domain that contains a virtual desktop infrastructure (VDI). The VDI uses non-persistent images and cloned virtual machine templates. VDI devices are members of the domain.

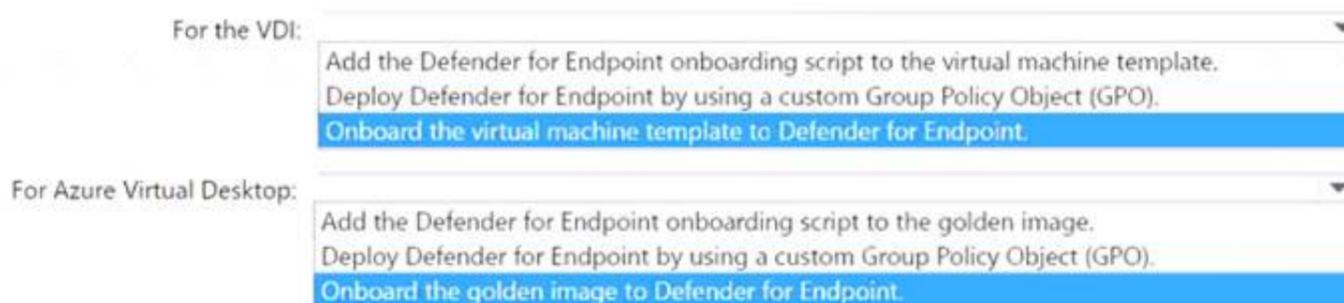
You have an Azure subscription that contains an Azure Virtual Desktop environment. The environment contains host pools that use a custom golden image. All the Azure Virtual Desktop deployments are members of a single Azure Active Directory Domain Services (Azure AD DS) domain.

You need to recommend a solution to deploy Microsoft Defender for Endpoint to the hosts. The solution must meet the following requirements:

- Ensure that the hosts are onboarded to Defender for Endpoint during the first startup sequence.
- Ensure that the Microsoft Defender 365 portal contains a single entry for each deployed VDI host.
- Minimize administrative effort.

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

**Answer Area**

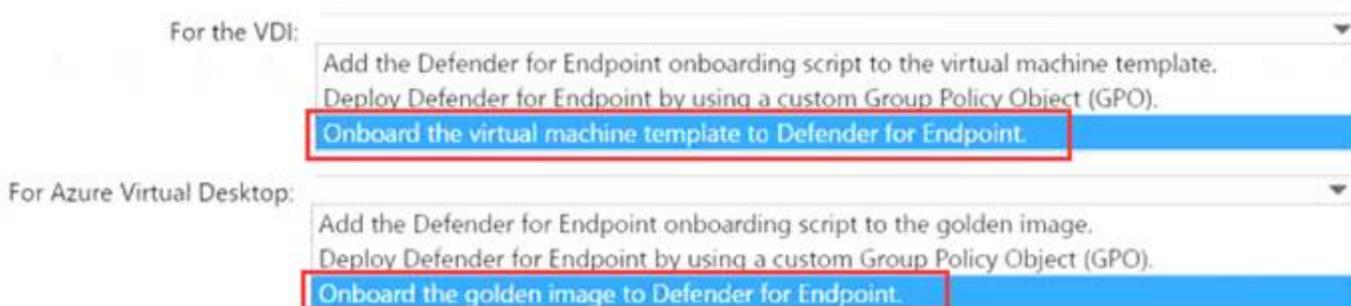


- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**



**NEW QUESTION 178**

- (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 for 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 179**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 183**

- (Exam Topic 3)

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The company plans to use Microsoft Information Protection for the PII data store in Azure. You need to recommend a solution to discover PII data at risk in the Azure resources.

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

To connect the Azure data sources to

Microsoft Information Protection:

<input type="checkbox"/> Azure Purview <input type="checkbox"/> Endpoint data loss prevention <input type="checkbox"/> Microsoft Defender for Cloud Apps <input type="checkbox"/> Microsoft Information Protection
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

To triage security alerts related to resources that contain PII data:

<input type="checkbox"/> Azure Monitor <input type="checkbox"/> Endpoint data loss prevention <input type="checkbox"/> Microsoft Defender for Cloud <input type="checkbox"/> Microsoft Defender for Cloud Apps
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Prioritize security actions by data sensitivity,

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection>. As to Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure resources as well): <https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azu>

**NEW QUESTION 188**

- (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 190**

- (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 194**

- (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.

**Answer Area**

For the SQL audit logs: [A Log Analytics workspace, Azure Application Insights, Microsoft Defender for SQL, Microsoft Sentinel]

For the Security logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for servers, Microsoft Sentinel]

For the App Service audit logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for App Service, Microsoft Sentinel]

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

For the SQL audit logs: [A Log Analytics workspace, Azure Application Insights, Microsoft Defender for SQL, Microsoft Sentinel]

For the Security logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for servers, Microsoft Sentinel]

For the App Service audit logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for App Service, Microsoft Sentinel]

**NEW QUESTION 196**

- (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.

<p><b>Features</b></p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Azure AD Password Protection</div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Extranet Smart Lockout (ESL)</div> <div style="border: 1px solid gray; padding: 2px;">Password hash synchronization</div>	<p><b>Answer Area</b></p> <div style="margin-bottom: 20px;">             For brute force password attacks: <input type="text"/></div> <div>             For leaked credentials: <input type="text"/></div>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<p><b>Features</b></p> <div style="border: 2px dashed green; padding: 2px; margin-bottom: 5px;">Azure AD Password Protection</div> <div style="border: 2px dashed green; padding: 2px; margin-bottom: 5px;">Extranet Smart Lockout (ESL)</div> <div style="border: 1px solid gray; padding: 2px;">Password hash synchronization</div>	<p><b>Answer Area</b></p> <div style="margin-bottom: 20px;">             For brute force password attacks: <div style="border: 1px solid red; padding: 2px;">Azure AD Password Protection</div> </div> <div>             For leaked credentials: <div style="border: 1px solid red; padding: 2px;">Extranet Smart Lockout (ESL)</div> </div>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**NEW QUESTION 198**

- (Exam Topic 3)

You have the following on-premises servers that run Windows Server:

- Two domain controllers in an Active Directory Domain Services (AD DS) domain
- Two application servers named Server1 and Server2 that run ASP.NET web apps
- A VPN server named Server3 that authenticates by using RADIUS and AD DS. End users use a VPN to access the web apps over the internet.

You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

What should you include in the recommendation?

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

**Answer: C**

#### NEW QUESTION 199

- (Exam Topic 3)

You are designing the encryption standards for data at rest for an Azure resource.

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

#### NEW QUESTION 201

- (Exam Topic 3)

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.

All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.

You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.

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

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

**Answer: AB**

#### Explanation:

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

#### NEW QUESTION 203

- (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 207

.....

## Relate Links

**100% Pass Your SC-100 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/SC-100-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>