

Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect



NEW QUESTION 1

- (Exam Topic 3)

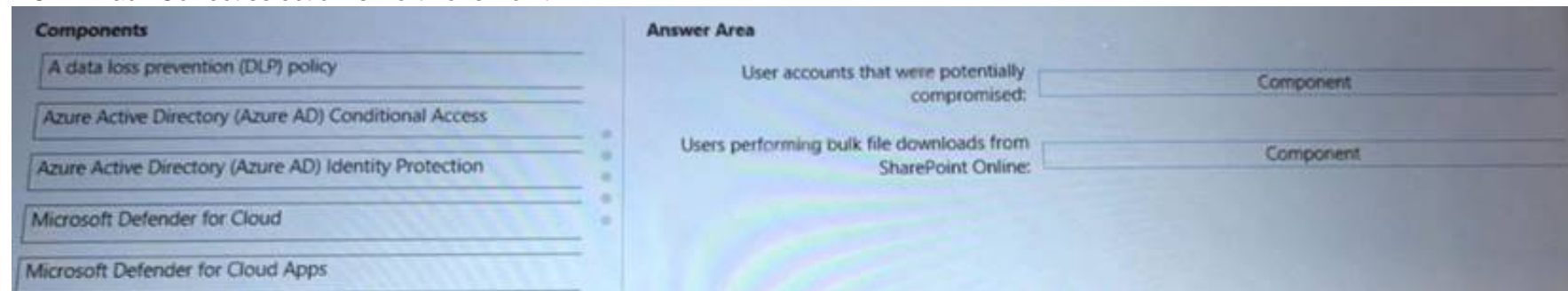
You have a Microsoft 365 subscription

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

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

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each Correct selection is worth one Point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 2

- (Exam Topic 3)

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

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 3

- (Exam Topic 3)

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 4

- (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 5

- (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 6

- (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 7

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation.

You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: BDE

Explanation:

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

NEW QUESTION 8

- (Exam Topic 3)

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD)

The customer plans to obtain an Azure subscription and provision several Azure resources. You need to evaluate the customer's security environment.

What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

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

Answer: D

Explanation:

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

NEW QUESTION 9

- (Exam Topic 3)

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

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

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

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

Answer Area

Deleted backups:

Soft delete of backups
A security PIN for critical operations
Encryption by using a customer-managed key
Multi-user authorization by using Resource Guard
Soft delete of backups

Disabled backups:

Multi-user authorization by using Resource Guard
A security PIN for critical operations
Encryption by using a customer-managed key
Multi-user authorization by using Resource Guard
Soft delete of backups

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Deleted backups:

Soft delete of backups
A security PIN for critical operations
Encryption by using a customer-managed key
Multi-user authorization by using Resource Guard
Soft delete of backups

Disabled backups:

Multi-user authorization by using Resource Guard
A security PIN for critical operations
Encryption by using a customer-managed key
Multi-user authorization by using Resource Guard
Soft delete of backups

NEW QUESTION 10

- (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 10

- (Exam Topic 3)

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

Answer Area

EDR:

Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD).
Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps.
Onboard the servers to Azure Arc.
Onboard the servers to Defender for Cloud.

SOAR:

Configure Microsoft Sentinel analytics rules.
Configure Microsoft Sentinel playbooks.
Configure regulatory compliance standards in Defender for Cloud.
Configure workflow automation in Defender for Cloud.

- A. Mastered
- B. Not Mastered

Answer: A

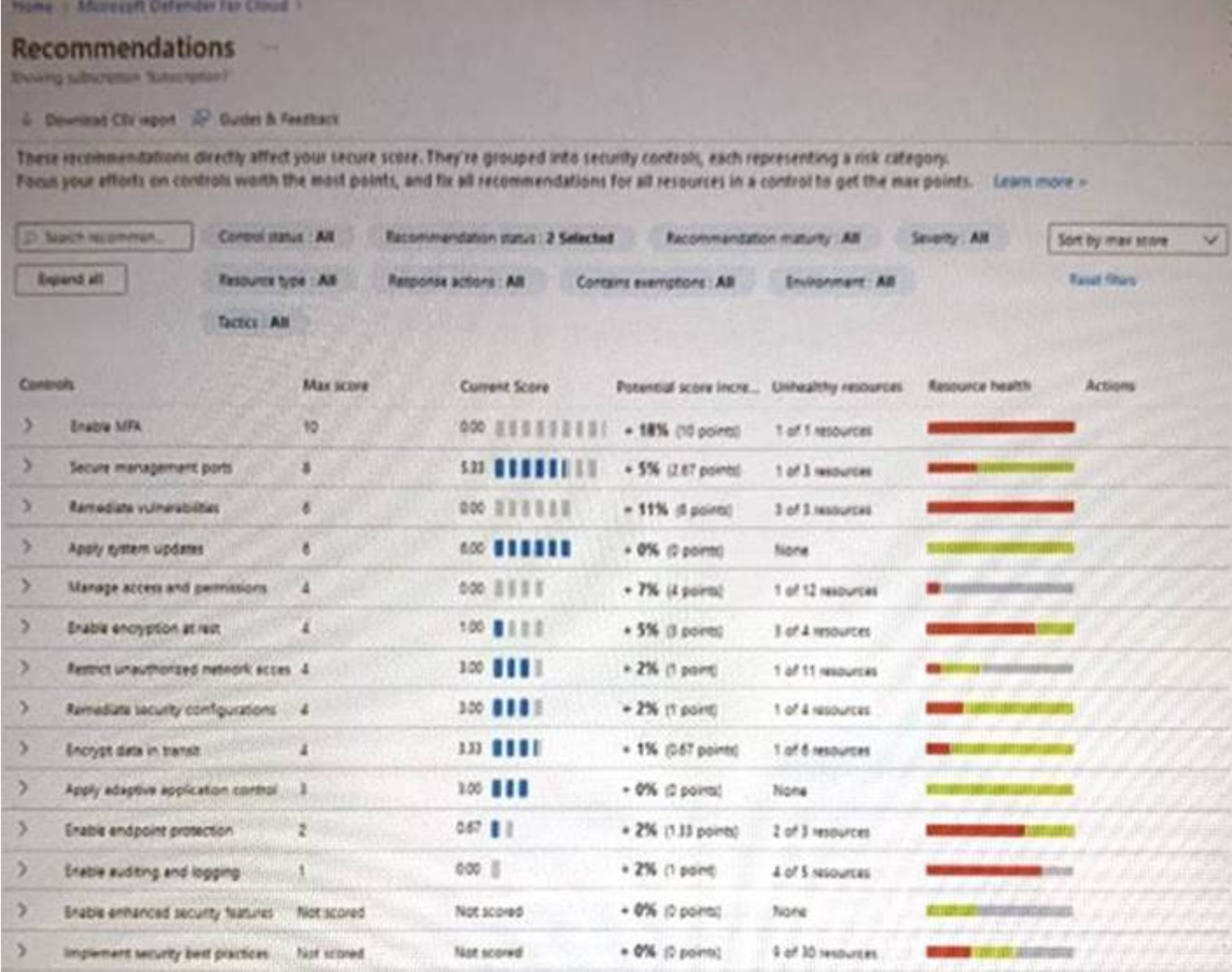
Explanation:

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 14

- (Exam Topic 3)

You open Microsoft Defender for Cloud as shown in the following exhibit.



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

Answer Area

To increase the score for the Restrict unauthorized network access control, implement [answer choice].

To increase the score for the Enable endpoint protection control, implement [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 15

- (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 17

- (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?

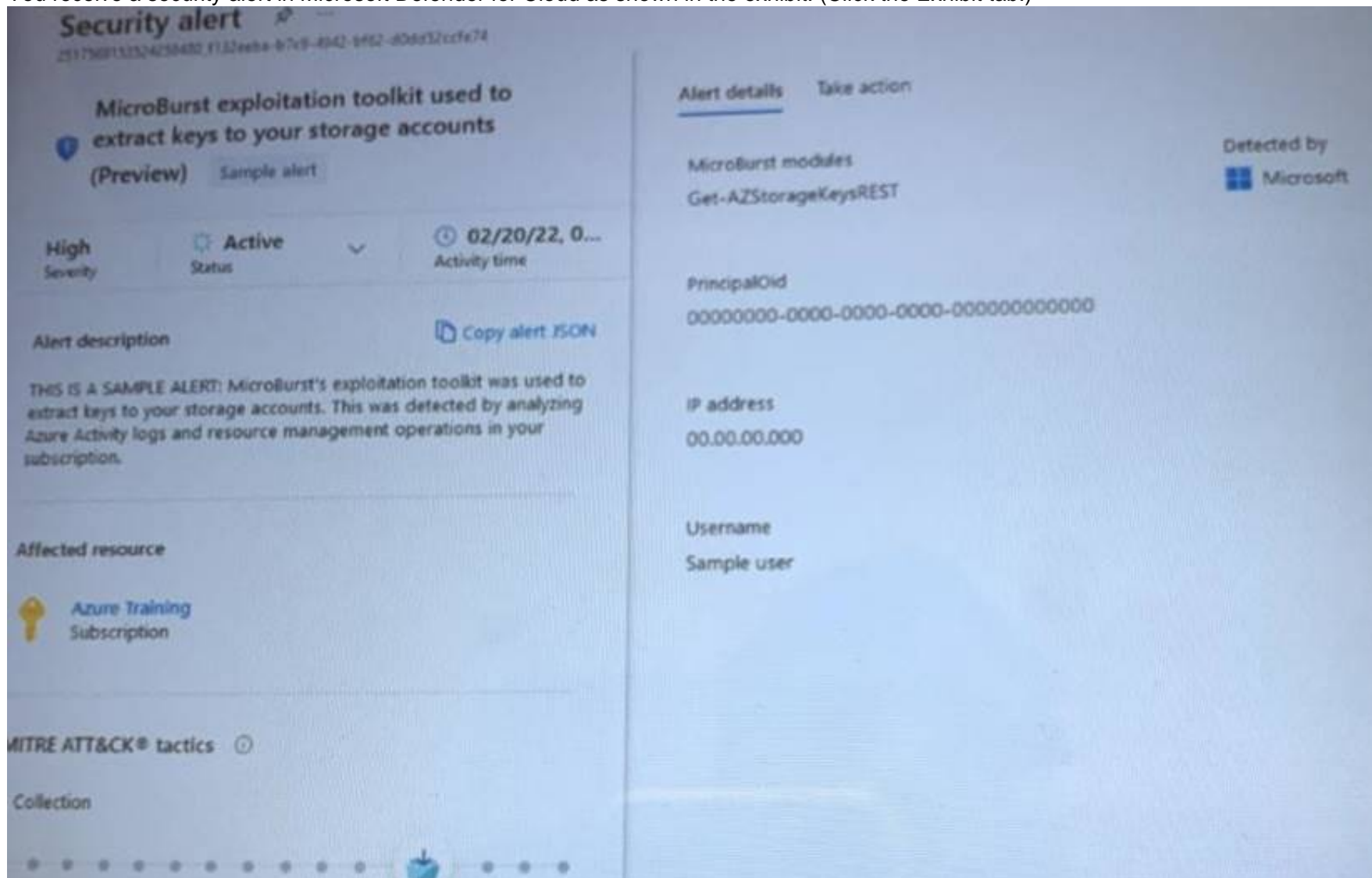
- A. the STRIDE model
- B. the DREAD model
- C. OWASP threat modeling

Answer: C

NEW QUESTION 19

- (Exam Topic 3)

You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



After remediating the threat which policy definition should you assign to prevent the threat from reoccurring?

- A. Storage account public access should be disallowed
- B. Azure Key Vault Managed HSM should have purge protection enabled
- C. Storage accounts should prevent shared key access
- D. Storage account keys should not be expired

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent>

NEW QUESTION 22

- (Exam Topic 3)

You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers. In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Linux containers deployed to Azure Container Registry
- B. Linux containers deployed to Azure Kubernetes Service (AKS)
- C. Windows containers deployed to Azure Container Registry
- D. Windows containers deployed to Azure Kubernetes Service (AKS)
- E. Linux containers deployed to Azure Container Instances

Answer: AC

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-sec> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabi>

NEW QUESTION 25

- (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 27

- (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 28

- (Exam Topic 3)

Azure subscription that uses Azure Storage.

The company plans to share specific blobs with vendors. You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be time-limited. What should you include in the recommendation?

- A. Create shared access signatures (SAS).
- B. Share the connection string of the access key.
- C. Configure private link connections.
- D. Configure encryption by using customer-managed keys (CMKs)

Answer: D

NEW QUESTION 32

- (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 36

- (Exam Topic 3)

You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.

You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

- A. Microsoft Information Protection
- B. Microsoft Defender for Endpoint
- C. Microsoft Sentinel
- D. Microsoft Endpoint Manager

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboa>

NEW QUESTION 38

- (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 39

- (Exam Topic 3)

You are planning the security levels for a security access strategy.

You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security level should you configure for each job role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Developer: Specialized security
 Enterprise security
 Privileged security
 Specialized security

Standard user: Enterprise security
 Enterprise security
 Privileged security
 Specialized security

IT administrator: Privileged security
 Enterprise security
 Privileged security
 Specialized security

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Developer: Specialized security
 Enterprise security
 Privileged security
 Specialized security

Standard user: Enterprise security
 Enterprise security
 Privileged security
 Specialized security

IT administrator: Privileged security
 Enterprise security
 Privileged security
 Specialized security

NEW QUESTION 44

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised administrator account cannot be used to delete the backups. What should you do?

- A. From a Recovery Services vault generate a security PIN for critical operations.
- B. From Azure Backup, configure multi-user authorization by using Resource Guard.
- C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.
- D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

Answer: B

NEW QUESTION 49

- (Exam Topic 3)

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

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

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

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

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

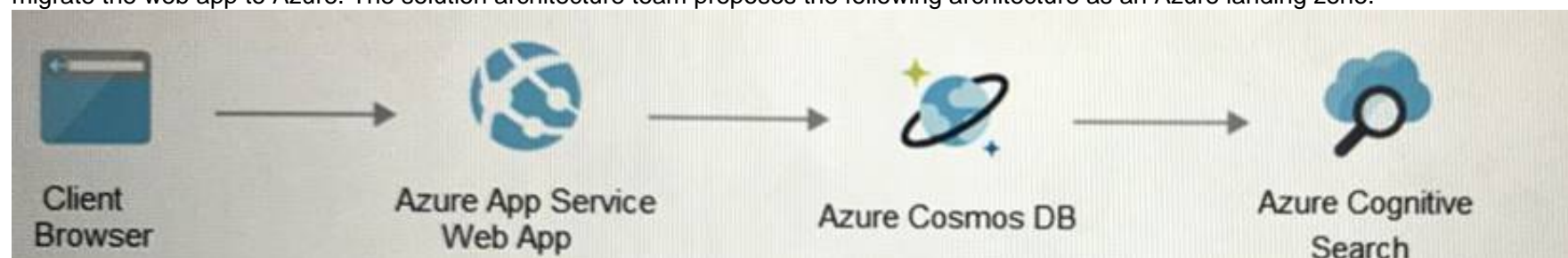
- A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
- B. Use the Azure Monitor agent with the multi-homing configuration.
- C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
- D. Create a custom collector that uses the Log Analytics agent.

Answer: BC

NEW QUESTION 54

- (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 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 59

- (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 64

- (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 65

- (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 67

- (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 69

- (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:

<input type="checkbox"/>	Azure AD application
<input type="checkbox"/>	Azure AD Application Proxy
<input type="checkbox"/>	Azure Application Gateway
<input type="checkbox"/>	A managed identity in Azure AD
<input type="checkbox"/>	Microsoft Defender for App

To implement access requests for App1, use:

<input type="checkbox"/>	An access package in Identity Governance
<input type="checkbox"/>	An access policy in Microsoft Defender for Cloud Apps
<input type="checkbox"/>	An access review in Identity Governance
<input type="checkbox"/>	Azure AD Conditional Access App Control
<input type="checkbox"/>	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 73

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

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

Answer: B

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

NEW QUESTION 78

- (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 79

- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud. The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?
A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, review the secure score recommendations.
C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
D. From Defender for Cloud, enable Defender for Cloud plans.

Answer: C

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

NEW QUESTION 83

- (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 86

- (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 87

- (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

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 89

- (Exam Topic 1)
You are evaluating the security of ClaimsApp.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE; Each correct selection is worth one point.

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	<input type="radio"/>	<input type="radio"/>
FD1 must be configured to have a certificate for claims.fabrikam.com.	<input type="radio"/>	<input type="radio"/>
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	<input type="radio"/>	<input checked="" type="radio"/>
FD1 must be configured to have a certificate for claims.fabrikam.com.	<input checked="" type="radio"/>	<input type="radio"/>
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 91

- (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 92

- (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 95

- (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 98

- (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 103

- (Exam Topic 3)

You have an Azure subscription.

You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar. Developers use Azure DevOps to deploy web apps to App Service Environments. When a new app is

deployed, a CNAME record for the app is registered in contoso.com.

You need to recommend a solution to secure the DNS record for each web app. The solution must meet the following requirements:

- Ensure that when an app is deleted, the CNAME record for the app is removed also
- Minimize administrative effort.

What should you include in the recommendation?

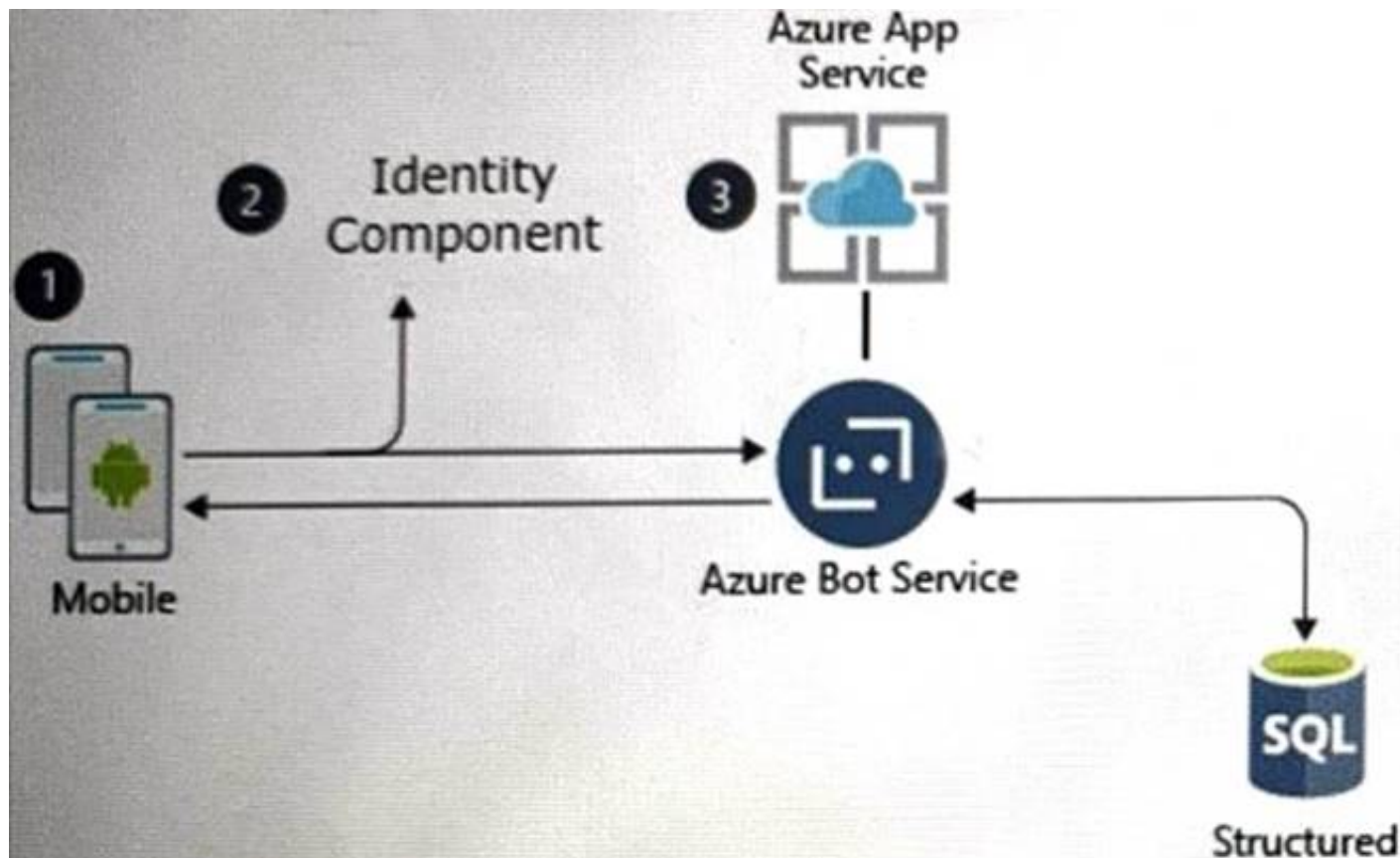
- A. Microsoft Defender for DevOps
- B. Microsoft Defender for App Service
- C. Microsoft Defender for Cloud Apps
- D. Microsoft Defender for DNS

Answer: C

NEW QUESTION 108

- (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

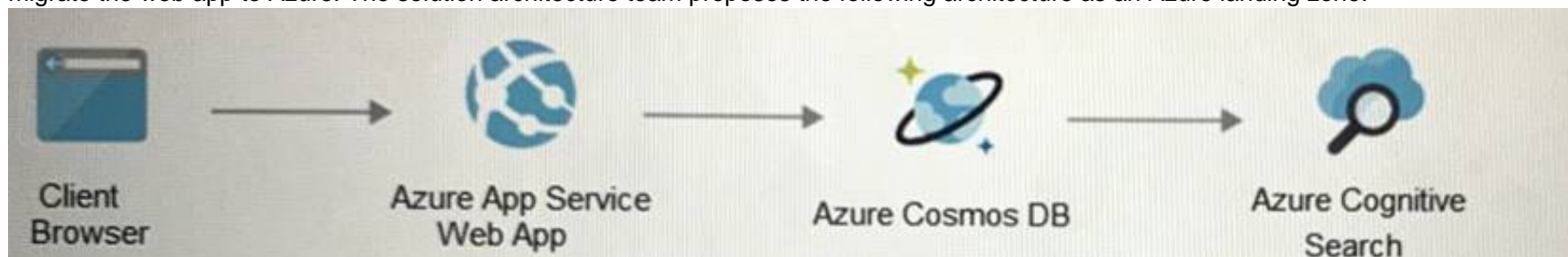
Explanation:

<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 112

- (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 Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 113

- (Exam Topic 3)

Your network contains an on-premises Active Directory Domain Services (AD 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

Identity Governance feature: Access reviews

Project team configuration: Azure AD Privileged Identity Management (PIM)
Entitlement management
Lifecycle workflows

Project team configuration: Enable group writeback for the existing synced groups.
Enable group writeback for the existing synced groups.
From Azure AD, create a new cloud-only security group for each project.
Azure AD, create a security group for each project and enable group writeback for each group.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Identity Governance feature: Access reviews

Project team configuration: Azure AD Privileged Identity Management (PIM)
Entitlement management
Lifecycle workflows

Project team configuration: Enable group writeback for the existing synced groups.
Enable group writeback for the existing synced groups.
From Azure AD, create a new cloud-only security group for each project.
Azure AD, create a security group for each project and enable group writeback for each group.

NEW QUESTION 114

- (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 115

- (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 118

- (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 123

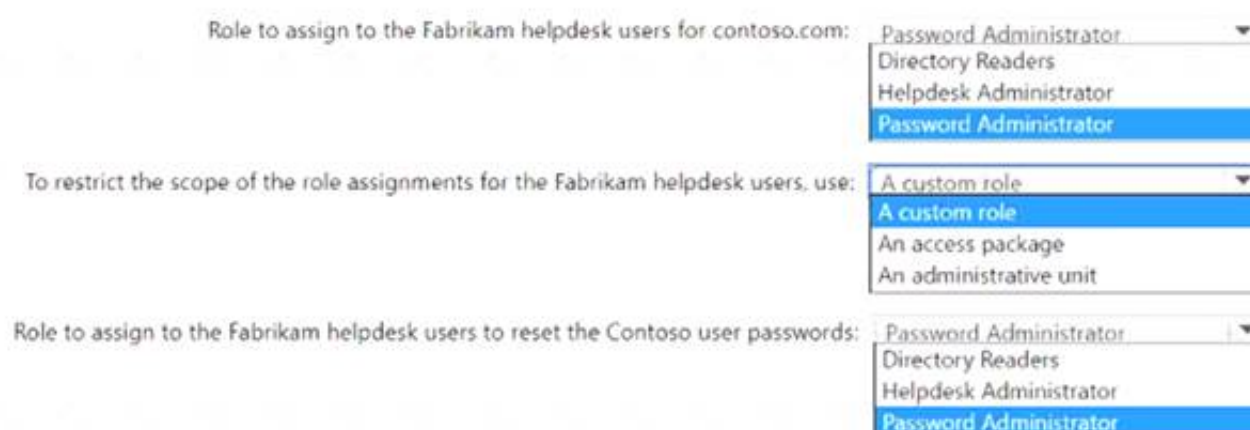
- (Exam Topic 3)

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

Role to assign to the Fabrikam helpdesk users for contoso.com:

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:

NEW QUESTION 124

- (Exam Topic 3)

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices. You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

- A. controlled folder access
- B. application isolation
- C. memory scanning
- D. machine isolation
- E. user isolation

Answer: D

NEW QUESTION 129

- (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 133

- (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 135

- (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:	<div>Encryption by using platform-managed keys</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>
Azure Storage:	<div>Immutable storage</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure Backup:	<div>Encryption by using platform-managed keys</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>
Azure Storage:	<div>Immutable storage</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>

NEW QUESTION 136

- (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 139

- (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:	<div>A threat intelligence connector</div> <div>Custom entity activities</div> <div>A playbook</div> <div>A threat detection rule</div> <div>A threat indicator</div> <div>A threat intelligence connector</div>
Automatically generate incidents:	<div>A threat detection rule</div> <div>Custom entity activities</div> <div>A playbook</div> <div>A threat detection rule</div> <div>A threat indicator</div> <div>A threat intelligence connector</div>

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

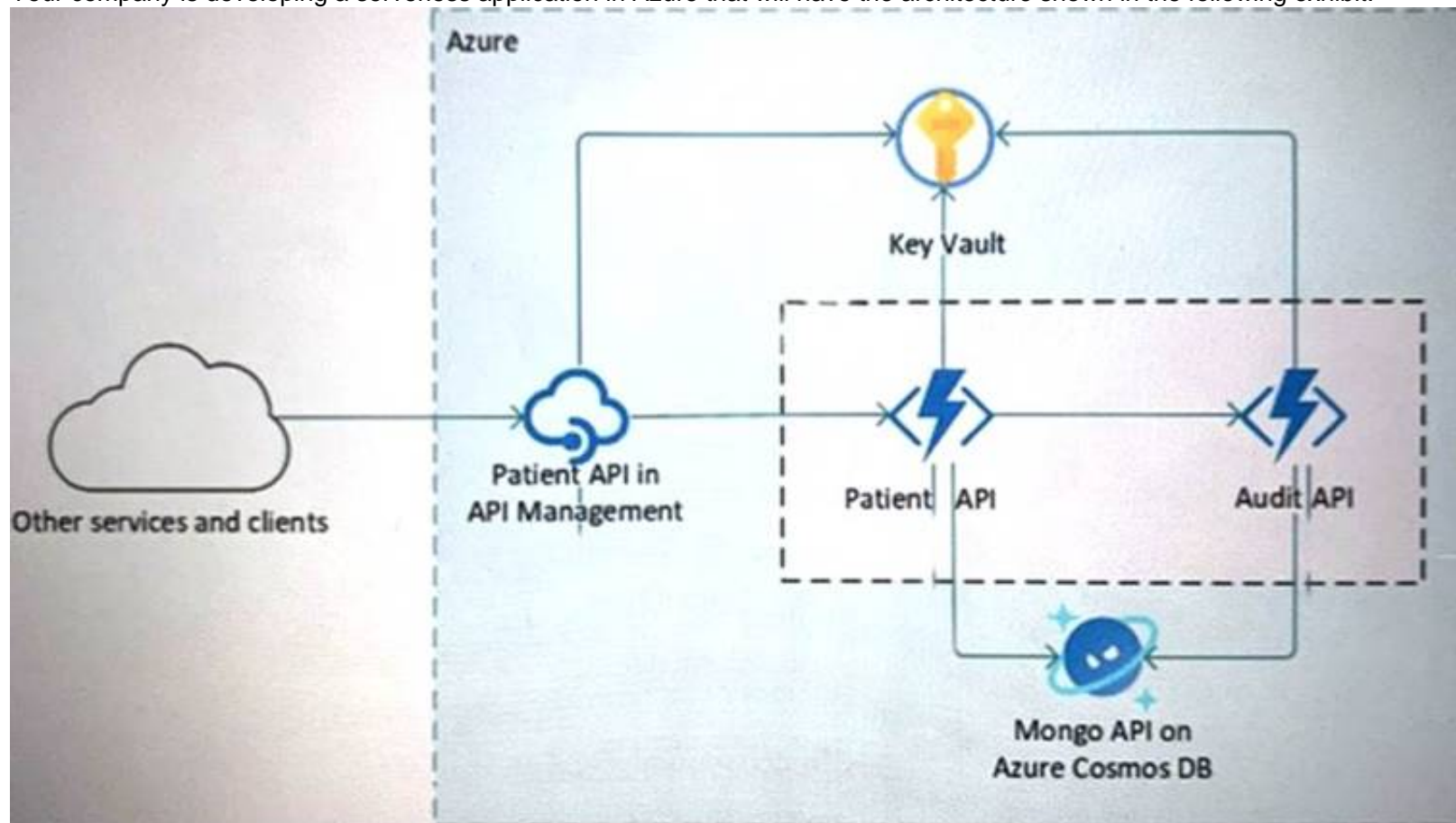
Answer Area



NEW QUESTION 144

- (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 146

- (Exam Topic 3)

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

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

NOTE: Each correct answer is worth one point.

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

Answer: AD

NEW QUESTION 151

- (Exam Topic 3)

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 153

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure.

The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.

The company's security policy prevents the use of personal devices for accessing company data and applications.

You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.

What should you include in the recommendation?

A. Migrate the on-premises applications to cloud-based applications.

B. Redesign the VPN infrastructure by adopting a split tunnel configuration.

C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.

D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop> <https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide> <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-c>

NEW QUESTION 155

- (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

For the VDI:

- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.**

For Azure Virtual Desktop:

- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.**

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

For the VDI:

- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.**

For Azure Virtual Desktop:

- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.**

NEW QUESTION 160

- (Exam Topic 3)

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

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

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

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

Answer Area

Manage NSG rules by using: Azure Bastion

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Manage NSG rules by using: Azure Bastion

Only allow SSH connections to the jump servers from: Any public IP addresses provided before the connection is established

NEW QUESTION 162

- (Exam Topic 3)

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

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

Answer: E

NEW QUESTION 167

- (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 169

- (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#honeypot-activity> The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

NEW QUESTION 173

- (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 178

- (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 179

- (Exam Topic 3)

Your company has an office in Seattle. The company has two Azure virtual machine scale sets hosted on different virtual networks. The company plans to contract developers in India. You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:

- Prevent exposing the public IP addresses of the virtual machines.
- Provide the ability to connect without using a VPN.
- Minimize costs.

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

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

Answer: AD

Explanation:

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

NEW QUESTION 182

- (Exam Topic 3)

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux. You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:

- Identify missing updates and insecure configurations.
- Use the Qualys engine. What should you use?

- A. Microsoft Defender for Servers
- B. Microsoft Defender Threat Intelligence (Defender TI)
- C. Microsoft Defender for Endpoint
- D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: A

NEW QUESTION 183

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

- A. data classification content explorer
- B. data loss prevention (DLP)
- C. eDiscovery
- D. Information Governance

Answer: B

NEW QUESTION 186

- (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
Build and test
Commit the code
Go to production
Operate
Plan and develop

Static application security testing: Plan and develop
Build and test
Commit the code
Go to production
Operate
Plan and develop

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Infrastructure scanning: Go to production
Build and test
~~Commit the code~~
Go to production
Operate
Plan and develop

Static application security testing: Plan and develop
Build and test
Commit the code
Go to production
Operate
Plan and develop

NEW QUESTION 191

- (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 195

- (Exam Topic 3)
Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Answer: C

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

NEW QUESTION 199

- (Exam Topic 3)

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

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

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

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

Answer: B

NEW QUESTION 203

- (Exam Topic 3)

You plan to automate the development and deployment of a Node.js-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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A close up of a text Description automatically generated

NEW QUESTION 208

- (Exam Topic 3)

You are designing a security operations strategy based on the Zero Trust framework.

You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts. What should you do?

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

Answer: C

NEW QUESTION 211

- (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:

For the Security logs:

A Log Analytics workspace
 Application Insights
 Microsoft Defender for servers
 Microsoft Sentinel

For the App Service audit logs:

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:

For the Security logs:

A Log Analytics workspace
 Application Insights
 Microsoft Defender for servers
 Microsoft Sentinel

For the App Service audit logs:

For the App Service audit logs:

A Log Analytics workspace
 Application Insights
 Microsoft Defender for App Service
 Microsoft Sentinel

NEW QUESTION 215

- (Exam Topic 3)

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface. What should you include in the recommendation?

- A. Azure Firewall Premium
- B. Azure Application Gateway Web Application Firewall (WAF)
- C. network security groups (NSGs)
- D. Azure Traffic Manager and application security groups

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection>

NEW QUESTION 220

- (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 222

- (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 225

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SC-100 Practice Exam Features:

- * SC-100 Questions and Answers Updated Frequently
- * SC-100 Practice Questions Verified by Expert Senior Certified Staff
- * SC-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-100 Practice Test Here](#)