Atmic Networks

CERTIFICATION EXAM SUPPORT

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE

> **Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.**

Stay connected with our support team
for the latest file updates and exam-related information.

www.atmicnetworks.com

Knowledge that moves beyond memorization.

Topic 1, Fabrikam, Inc Case Study 1

OverView

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment

Fabrikam has the following Azure resources:

- An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com
- A single Azure subscription named Sub1
- A virtual network named Vnet1 in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled
- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-.

- An Azure AD tenant named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

- Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

- ClaimsApp will be deployed to Azure App Service instances that connect to Vnetl and Vnet2.
- Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- Azure DevTest labs will be used by developers for testing.
- All the application code must be stored in GitHub Enterprise.
- Azure Pipelines will be used to manage application deployments.

- All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- Internet-accessible applications must prevent connections that originate in North Korea.
- Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
- Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers;

- Every month, the membership of the ContosoDevelopers group must be verified.
- The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Question: 1

You need to recommend a solution to meet the security requirements for the InfraSec group.

What should you use to delegate the access?

A. a subscription

B. a custom role-based access control (RBAC) role

C. a resource group

D. a management group

Answer: B

Explanation:

Question: 2

You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?

A. Azure Key Vault

B. GitHub Advanced Security

C. Application Insights in Azure Monitor

D. Azure DevTest Labs

Answer: B

Explanation:

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

Question: 3

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation? (Choose Two)

A. Onboard the virtual machines to Microsoft Defender for Endpoint.

B. Onboard the virtual machines to Azure Arc.

C. Create a device compliance policy in Microsoft Endpoint Manager.

D. Enable the Qualys scanner in Defender for Cloud.

Answer: A, D

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-

3?view=o365-worldwide

Question: 4

HOTSPOT

What should you create in Azure AD to meet the Contoso developer requirements?

Account type for the developers: I

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

Component in Identity Governance: I

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

Answer:

Explanation:

Box 1: A synced user account -

Need to use a synched user account.

Box 2: An access review

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 5

HOTSPOT

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 ^ No

Statements	
FD1 can be used to protect all the instances of ClaimsApp.	
FD1 must be configured to have a certificate for daims.fabrikam.com.	
ToMoMnnKtonsMnNomK^^	0

Answer:

Explanation:

No

Yes

Yes

Question: 6

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-enclaves

Question: 7

HOTSPOT

You need to recommend a solution to meet the AWS 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 the AWS EC2 instances: [1] Azure Blueprints I
Defender for Cloud 1 1
Microsoft Defender for Cloud Apps \
1 Microsoft Defender for servers 1
(Microsoft Endpoint Manager I
[Microsoft Sentinel 1

For the AWS service logs: Azure Blueprints 1 1
Defender for Cloud
Microsoft Defender for Cloud Apps I Microsoft Defender
for servers I Microsoft Endpoint Manager
I Microsoft Sentinel

Answer:

Explanation:

Question: 8

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

www.atmicnetworks.com

Question: 9

HOTSPOT

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 |^H^^H^^^^^^^^Bi^B 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)

Answer:

Explanation:

A Private endpoint

A managed identity

Question: 10

HOTSPOT

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: I

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

To exclude TestRG from the compliance assessment I

- Edit an Azure bluepnnt
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition

www.atmicnetworks.com

Update an Azure policy assignment

Answer:

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-exclusion

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

Topic 2, Litware, inc. Case Study 2

Overview

Litware, inc. is a financial services company that has main offices in New York and San Francisco. litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD D%) forest named Utvvare.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Planned Changes

Litware plans to implement the following changes:

- Create a management group hierarchy for each Azure AD tenant.

- Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.
- Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Business Requirements

Litware identifies the following business requirements:

- Minimize any additional on-premises infrastructure.
- Minimize the operational costs associated with administrative overhead.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

- Enable the management of on-premises resources from Azure, including the following:
- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.
- Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAK) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOQ by using Microsoft Sentinel.

Identity Requirements

Litware identifies the following identity requirements:

- Detect brute force attacks that directly target AD DS user accounts.
- Implement leaked credential detection in the Azure AD tenant of Litware.
- Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
- Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for.
- The management of group properties, membership, and licensing « The management of user properties, passwords, and licensing

- The delegation of user management based on business units.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

- insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.

- Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.

- Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

- Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
- Provide a secure score scoped to the landing zone.

- Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
- Minimize the possibility of data exfiltration.

- Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

- Be created in a dedicated subscription.

- Use a DNS namespace of litware.com.

Application Security Requirements

Litware identifies the following application security requirements:

- Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

- Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Question: 11

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-on-premises-apps

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

Question: 12

You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.

What should you configure for each landing zone?

A. Azure DDoS Protection Standard

B. an Azure Private DNS zone

C. Microsoft Defender for Cloud

D. an ExpressRoute gateway

Answer: D

Explanation:

One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive.

Given the landing zone requirements of

1) "Use a DNS namespace of litware.com"

2) "Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints"

Question: 13

HOTSPOT

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.

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

Answer:

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-attack-ldap-external-id-2004

Question: 16

HOTSPOT

You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

For the delegated management of users and groups, use:

AD DS organizational units
Azure AD administrative units
Custom Azure AD roles

To ensure that you can perform leaked credential detection:

Enable password hash synchronization in the Azure AD Connect deployment
Enable Security defaults in the Azure AD tenant of Litware
Replace pass-through authentication with Active Directory Federation Services

Answer:

Explanation:

For the delegated management of users and groups, use;

Azure AD administrative units

TO ensure that you can perform leaked credential detection;

Enable password hash synchronization in the Azure AD Connect deployment

Question: 17

HOTSPOT

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.

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

Answer: >

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.

Question: 18

HOTSPOT

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)

Answer:

Evaluate regulatory compliance of cloud resources by assigning:	Azure Policy initiatives to management grot
Evaluate regulatory compliance of on-premises resources by using:	Azure Arc

Question: 19

You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.

Which two services should you leverage in the strategy? Each correct answer presents part of the solution.

NOTE; Each correct selection is worth one point.

A. Azure AD Conditional Access

B. Microsoft Defender for Cloud Apps

C. Microsoft Defender for Cloud

D. Microsoft Defender for Endpoint

E. access reviews in Azure AD

Answer: B, C

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional- access-session#conditional-access-application-control

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cloud-application-security

Topic 3, Mix Questions

Question: 20

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. Azure SQL Managed Instance

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

D. SQL Server on Azure Virtual Machines

Answer: C

Explanation:

Question: 21

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

What should you include in the recommendation?

A. Apply read-only locks on the storage accounts.

B. Set the AllowSharcdKeyAccess property to false.

C. Set the AllowBlobPublicAcccss property to false.

D. Configure automated key rotation.

Answer: A

Explanation:https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Question: 22

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 t\me-Vim\ted. 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

Explanation:

Question: 23

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: B, C

Explanation:

https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs

Question: 24

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: D, E

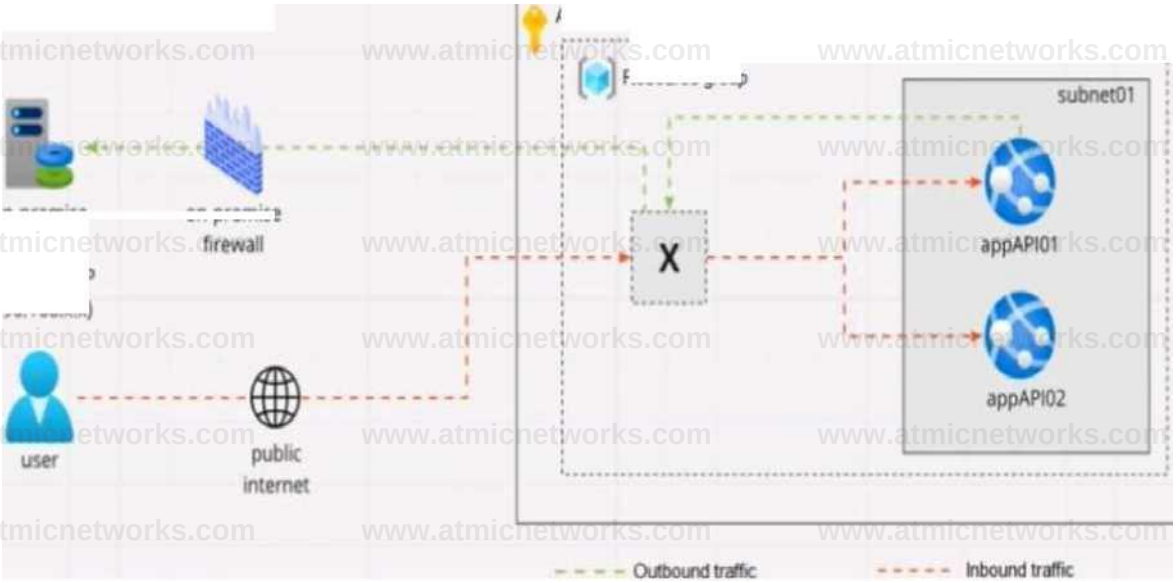
Explanation:

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

Question: 25

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)

You need to recommend a solution to ensure that the web apps can communicate with the onpremises application



server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Application Gateway v2 with user-defined routes (UDRs).

C. Azure Front Door with Azure Web Application Firewall (WAF)

D. Azure Firewall with policy rule sets

Answer: C

Explanation:

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

Question: 26

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-worldwide#configure-web-content-filtering-policies

Question: 27

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	VNeti, VNet2
VNet!	Windows virtual machines	Hub VNet
VN«2	Linux virtual machines	Hub VNet
VNetS	Windows virtual machine scale sets	VNeti
VNeU	Linux virtual machine scale sets	VNeB

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:

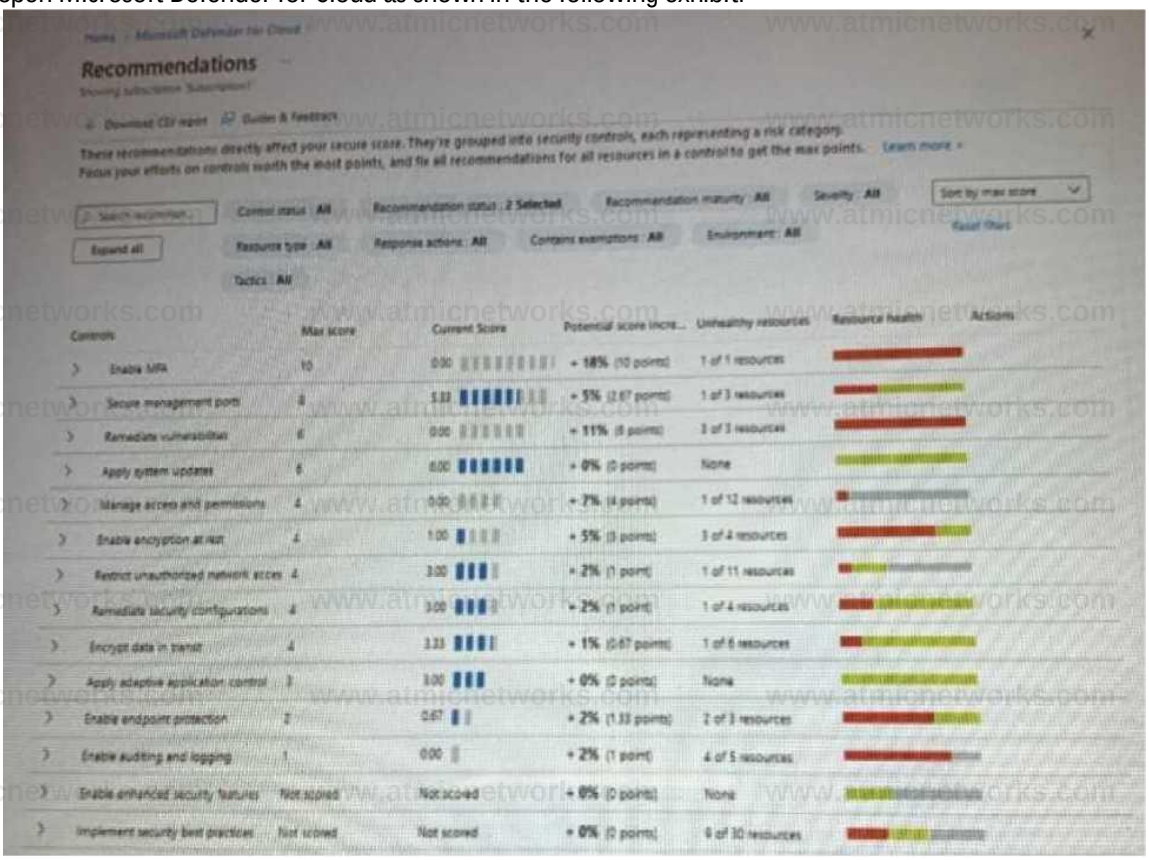
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

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

Question: 28

HOTSPOT

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.

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

Azure Active Directory (Azure AD) Conditional Access policies
Azure Web Application Firewall (WAF)
network security groups (NSGs)

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

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

Answer:

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

Question: 29

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-with-built-in-azure-blueprints/

Question: 31

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: D, E

Explanation:

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

Question: 32

HOTSPOT

You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:

- Windows 11 devices managed by Microsoft Intune
- Azure Storage accounts
- Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

Windows 11 devices:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure virtual machines:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure Storage accounts:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Answer:

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-security-requirements-for-storage-workloads

www.atmicnetworks.com

Question: 33

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: A, C

Explanation:

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

Question: 34

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

- Access to storage accounts with firewall and virtual network configurations should be restricted,
- Storage accounts should restrict network access using virtual network rules.
- Storage account should use a private link connection.
- Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations. What should

you recommend?

A. Azure Storage Analytics

B. Azure Network Watcher

C. Microsoft Sentinel

D. Azure Policy

Answer: D

Explanation:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept

https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

Question: 35

You have 50 Azure subscriptions.

You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.

NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.

B. Assign a policy to each subscription.

C. Assign a policy to a management group.

D. Assign an initiative to each subscription.

E. Assign a blueprint to each subscription.

F. Assign a blueprint to a management group.

Answer: AF

Explanation:

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

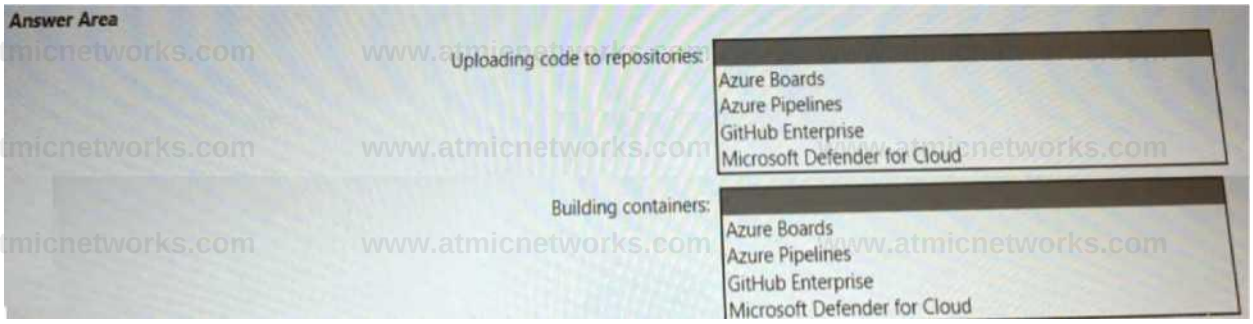
Question: 36

HOTSPOT

Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:

Uploading the code to repositories Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.



Answer:

Explanation:

https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about- github-advanced-security

https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific- samples/azdo-container-dev-test-release/

Question: 37

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

Explanation:

Question: 38

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: A, E

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

Question: 39

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

Question: 40

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: A, C

Explanation:

https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-security-requirements-for-containers

https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabilities-for-running-images

Question: 41

HOTSPOT

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:

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-create

Question: 42

Your company has an on-premises network and an Azure subscription.

The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.

You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.

You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.

What should you include in the recommendation?

A. a private endpoint

B. hybrid connections

C. virtual network NAT gateway integration

D. virtual network integration

Answer: B

Explanation:

https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

Question: 43

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

Question: 45

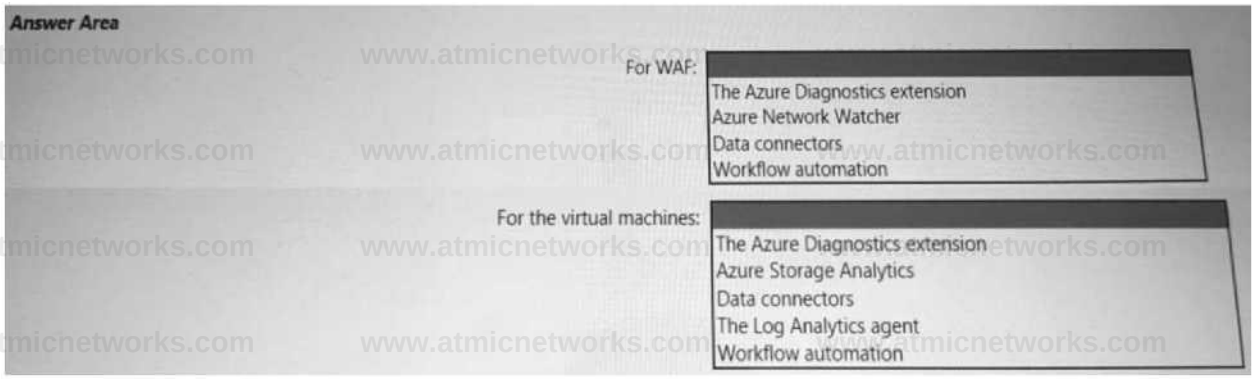
HOTSPOT

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.

You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

- Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
- Use Defender for Cloud to review alerts from the virtual machines.

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



Answer:

Explanation:

For WAF: Data connectors

For the virtual machines: The Loq Analytics agent

Question: 46

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-eventhub/ba-p/2307029

Question: 47

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-containers?tabs=aws-eks

Question: 48

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

Question: 50

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: B

Explanation:

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged- access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration

Question: 51

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

Question: 52

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-front-door-instance

Question: 53

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

Explanation:

Question: 54

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-front-door-instance

Question: 55

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

Question: 56

Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app.

You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection. What should you include in the recommendation?

A. interactive application security testing (IAST)

B. static application security testing (SAST)

C. runtime application se/f-protection (RASP)

D. dynamic application security testing (DAST)

Answer: D

Explanation:

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

Question: 57

DRAG DROP

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	Answer Area	
Files and emails	SharePoint Online:	Scope
Groups and sites	Microsoft Tearns:	Scope
Schematized data assets	Exchange Online:	Scope

Answer:

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

www.atmicnetworks.com

Question: 58

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 attach 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

Question: 59

HOTSPOT

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:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

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

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer:

Explanation:

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

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

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

www.atmicnetworks.com

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=azuresql

Question: 60

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.

www.atmicnetworks.com

Question: 61

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-cloud-apps/ba-p/2835842

Question: 62

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 ofline backups to Azure Data Box.

D. Encrypt backups by using customer-managed keys (CMKs).

E. Enable soft delete for backups.

Answer: A, B

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.

Question: 63

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-

location

https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules

Question: 64

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity.

You are informed about incidents that relate to compromised identities.

You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

A. standalone sensors

B. honeytoken entity tags

C. sensitivity labels

D. custom user tags

Answer: B

Explanation:

https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken- activity

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

Question: 65

You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events. What should you recommend using in Microsoft Sentinel?

A. playbooks

B. workbooks

C. notebooks

D. threat intelligence

Answer: B

Explanation:

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

Question: 66

Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.

The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.

Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.

You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.

Which three actions should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.

B. Implement Azure Firewall to restrict host pool outbound access.

C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

D. Migrate from the Remote Desktop server to Azure Virtual Desktop.

E. Deploy a Remote Desktop server to an Azure region located in France.

Answer: BCD

Explanation:

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

www.atmicnetworks.com

Question: 67

HOTSPOT

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

- Azure IoT Edge devices
- AWS EC2 instances

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

Answer Area

For the IoT Edge devices:

For the AWS EC2 instances:

Azure Arc
Microsoft Defender for Cloud
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for IoT

Answer:

For the AWS EC2 instances:

Azure Arc only
Microsoft Defender for Cloud and Azure Arc
Microsoft Defender for Cloud Apps only
Microsoft Defender for Cloud only
Microsoft Defender for Endpoint and Azure Arc
Microsoft Defender for Endpoint only

Explanation:

For the IoT Edge device* Microsoft Defender for IoT

For the AWS EC2 instance* Microsoft Defender for Cloud and Azure Arc

https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations

Question: 68

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

Question: 69

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

A. service tags in network security groups (NSGs)

B. managed rule sets in Azure Web Application Firewall (WAF) policies

C. inbound rules in network security groups (NSGs)

D. firewall rules for the storage account

E. inbound rules in Azure Firewall

Answer: D

Explanation:

Question: 70

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-vulnerability-management?view=o365-worldwide)

Question: 71

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

Question: 72

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-elements/1b-elements

https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started?source=recommendations

Question: 73

Your company is moving a big data solution to Azure.

The company plans to use the following storage workloads:

- Azure Storage blob containers
- Azure Data Lake Storage Gen2
- Azure Storage file shares
- Azure Disk Storage

Which two storage workloads support authentication by using Azure Active Directory (Azure AD)?

Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Disk Storage

B. Azure Storage blob containers

C. Azure Storage file shares

D. Azure Data Lake Storage Gen2

Answer: BD

Explanation:

https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory

https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure- datalake-gen2-sp-access

Question: 74

HOTSPOT

You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

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

Data security: ▼

Access keys stored in Azure Key Vault Automation Contributor built-in role

Azure Private Link with network service tags

Azure Web Application Firewall rules with network service tags

Network access control:1 Access keys stored in Azure Key Vault Automation Contributor built-in role

Azure Private Link with network service tags

Azure Web Application Firewall rules with network service tags

Answer:

Explanation:

Data Security = Access Keys stored in Azure Key Vault

Network access control = Azure Private Link with network service tags

https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security

Question: 75

You are evaluating an Azure environment for compliance.

You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.

Which effect should you use in Azure Policy?

A. Deny

B. Disabled

C. Modify

D. Append

Answer: B

Explanation:

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

Question: 76

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

Question: 78

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

Question: 79

You have Microsoft Defender for Cloud assigned to Azure management groups.

You have a Microsoft Sentinel deployment.

During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. workload protections in Defender for Cloud

B. threat intelligence reports in Defender for Cloud

C. Microsoft Sentinel notebooks

D. Microsoft Sentinel threat intelligence workbooks

Answer: B, D

Explanation:

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

Question: 80

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/select-types-of-rules-to-create#windows-defender-application-control-policy- rules

Question: 81

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-regulatory-compliance-standards-are-available-in-defender-for-cloud

Question: 82

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.

Question: 83

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.

Question: 84

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

Question: 86

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/security-compliance-toolkit-10

Question: 87

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware.

The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Endpoint reports the endpoints as compliant.

B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. The client access tokens are refreshed.

Answer: C, D

Explanation:

https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/

https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

Question: 88

HOTSPOT

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.

www.atmicnetworks.com

Answer Area

For the SQL audit logs:

For the Security logs:

A Log Analytics workspace
Azure Application Insights
Microsoft Defender for SQL
Microsoft Sentinel

For the Security logs:

For the App Service audit 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

Answer:

Explanation:

Microsoft Defender for SQL

A Log Analytics workspace

Microsoft Sentinel

Question: 89

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

Explanation:

Question: 90

HOTSPOT

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 HH^^^^^^H^^^MI^HH^^^^^^^^^I

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 ^^^^M^^^^M^^^^^H^H^^^^^^^H

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

Answer:

Explanation:

EDR: Onboard the servers to Defender for Cloud.

SOAR: Configure Microsoft Sentinel playbooks.

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

Question: 91

Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.

You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.

What should you include in the recommendation?

A. Use geo-redundant storage (GRS).

B. Use customer-managed keys (CMKs) for encryption.

C. Require PINs to disable backups.

D. Implement Azure Site Recovery replication.

Answer: C

Explanation:

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

Question: 92

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 Intune

Answer: D

Explanation:

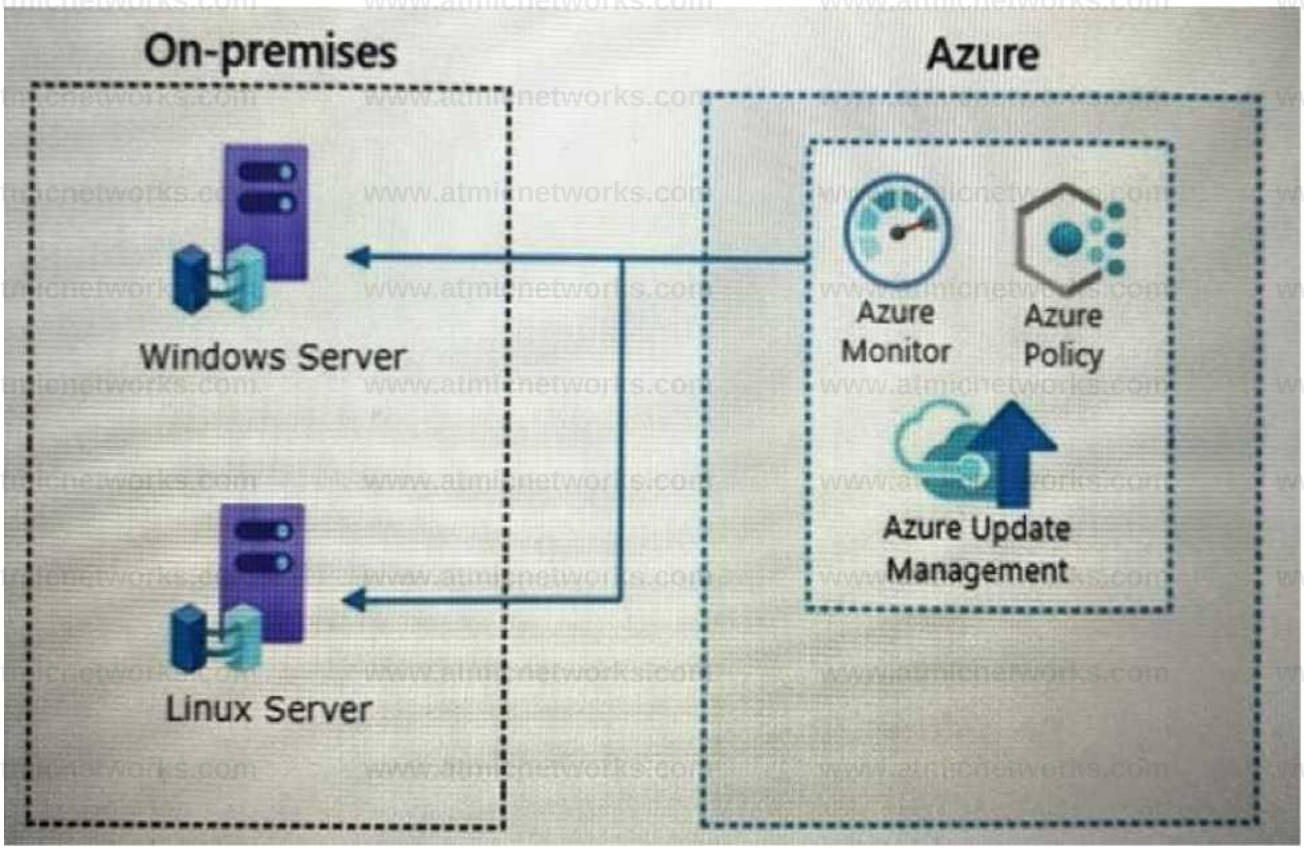
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

Question: 93

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:

Govern virtual machines and servers across multiple environments.
Enforce standards for all the resources across all the environment across the Azure policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

A. Azure VPN Gateway
B. guest configuration in Azure Policy
C. on-premises data gateway
D. Azure Bastion
E. Azure Arc

Answer: B, E

Explanation:

https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

Question: 94

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.

Question: 95

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

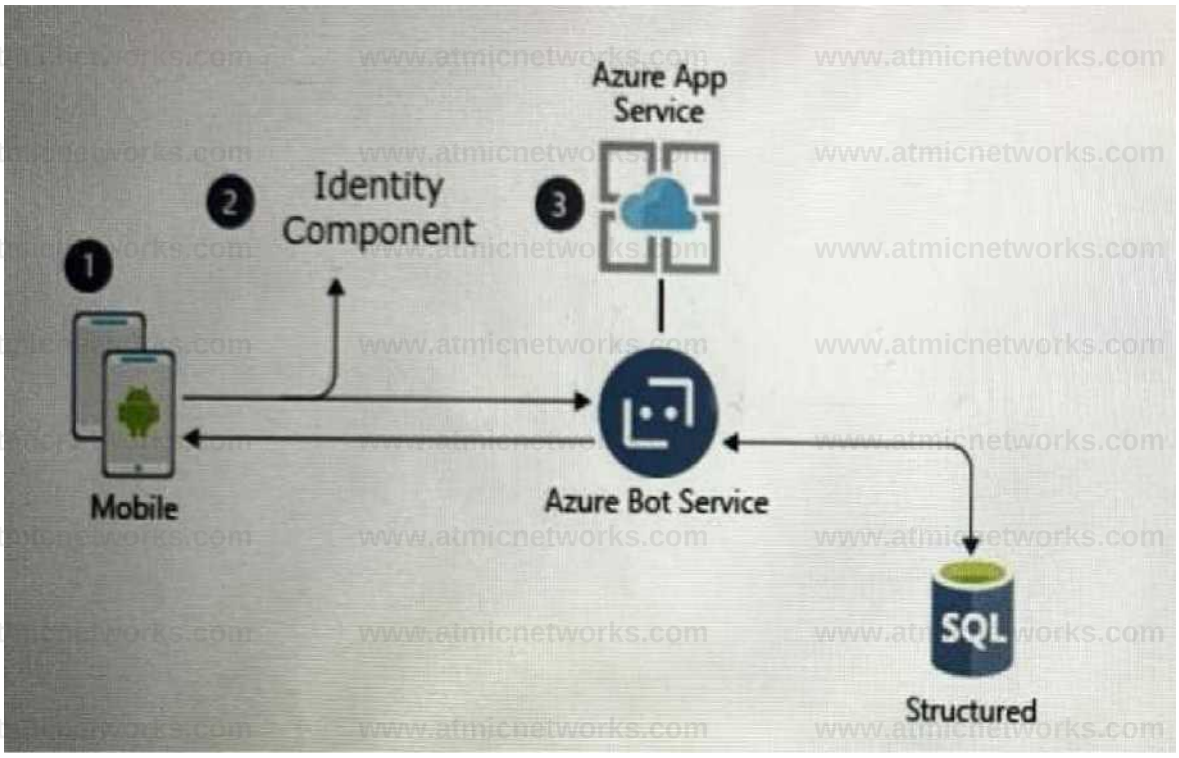
Explanation:

(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

Question: 96

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

Question: 97

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs.

What should you include in the recommendation?

A. Microsoft 365 Defender

B. Microsoft Defender for Cloud

C. Microsoft Defender for Cloud Apps

D. Microsoft Sentinel

Answer: D

Explanation:

Question: 98

You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Add Microsoft Sentinel data connectors.

B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.

C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.

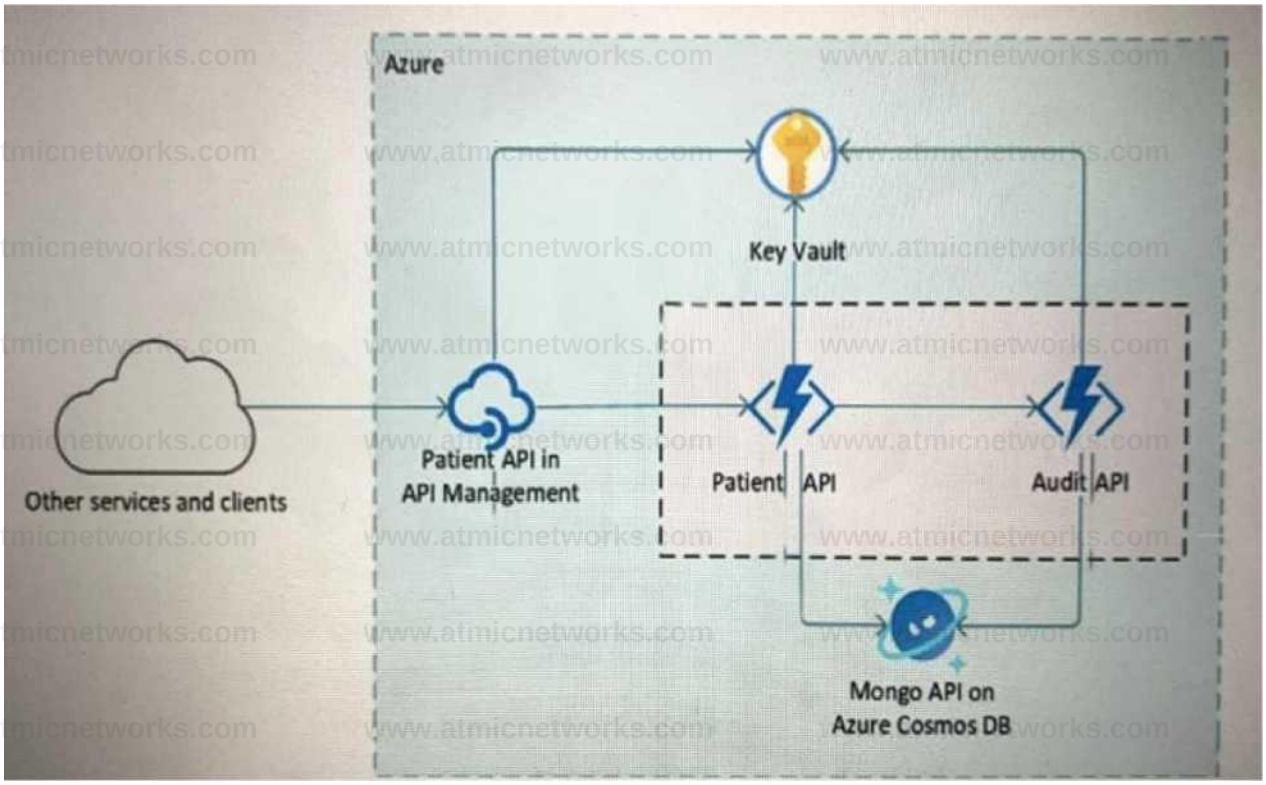
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Answer: C

Explanation:

Question: 99

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

Question: 100

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: A, B

Explanation:

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

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate. Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities 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?view=o365-worldwide#sensitivity-labels

Question: 101

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

Question: 102

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 based on HTTP headers that have the Front Door ID.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access- to-my-backend-to-only-azure-front-door-

Question: 103

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

Question: 104

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

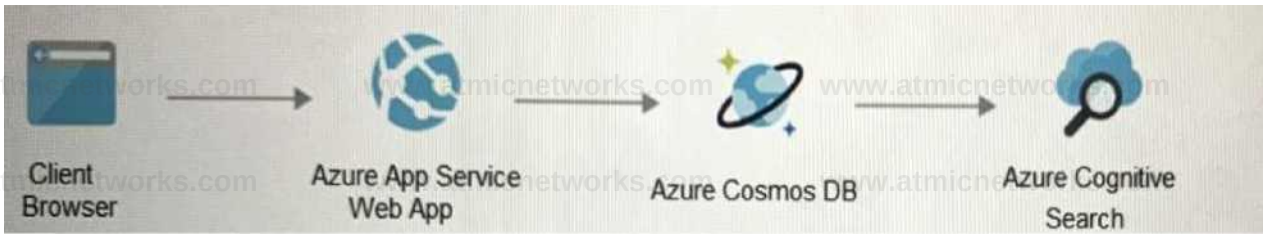
Answer: A

Explanation:

https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Question: 105

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

Question: 106

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-recommendations

Question: 107

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

All the on-premises servers in the perimeter network are prevented from connecting directly to the internet.

The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

- Ensure that the security operations team can access the security logs and the operation logs.

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

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

A. Azure Active Directory (Azure AD) Conditional Access policies

B. a custom collector that uses the Log Analytics agent

C. resource-based role-based access control (RBAC)

D. the Azure Monitor agent

Answer: C, D

Explanation:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

Question: 108

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

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Key Vault to store credentials.

A. Yes

B. No

Answer: B

Explanation:

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

Question: 109

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: B

Explanation:

Question: 110

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

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

Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 111

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

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

Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

Question: 112

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-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration

Question: 113

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-regulatory-compliance-standards-are-available-in-defender-for-cloud

Question: 114

HOTSPOT

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

Answer:

Explanation:

Answer Area

Azure Backup: Encryption by using platform-managed keys
*

Azure Storage ["immutable storage
^

Question: 116

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: A

Explanation:

Question: 117

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

Explanation:

Question: 118

HOTSPOT

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

Answer:

Explanation:

Answer Area

Infrastructure scanning: Go to production

Static application security testing Plan and develop

Question: 119

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: A, C, E

Explanation:

Question: 120

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

Explanation:

Question: 121

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

Explanation:

Question: 122

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

A. Disable Microsoft OneDnve sync and Exchange ActiveSync.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. From Microsoft Defender for Endpoint perform a security scan.

Answer: A

Explanation:

Question: 123

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: A

Explanation:

Question: 124

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online. SharePoint Online, and Teams m near-real-lime (NRT) in response to the following Azure AD events:

- A user account is disabled or deleted
- The password of a user is changed or reset.
- All the refresh tokens for a user are revoked
- Multi-factor authentication (MFA) is enabled for a user

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

NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. a sign-in risk policy

C. Azure AD Privileged Identity Management (PIM)

D. Conditional Access

E. Azure AD Application Proxy

Answer: A, D

Explanation:

Question: 126

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

Explanation:

Question: 127

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

Explanation:

Question: 128

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: B

Explanation:

Question: 129

HOTSPOT

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

Answer:

Explanation:

Answer Area

An attacker attempts to exfiltrate data to external websites: Microsoft Defender for Identity

An attacker attempts lateral movement across domain-joined computers: Microsoft Defender for Identity

Question: 130

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: A, B, D

Explanation:

www.atmicnetworks.com

Question: 131

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

Explanation:

Question: 132

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure.

What should you include in the recommendation?

A. the Azure landing zone accelerator

B. the Azure Will-Architected Framework

C. Azure Security Benchmark v3

D. Azure Advisor

Answer: A

Explanation:

Question: 133

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: A, D

Explanation:

Question: 134

You have an Azure subscription.

You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar Developers use Azure DevOps to deploy web apps to App Service Environments- When a new app is deployed, a CNAME record for the app is registered in contoso.com.

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

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

What should you include in the recommendation?

A. Microsoft Defender for DevOps

B. Microsoft Defender foe App Service

C. Microsoft Defender for Cloud Apps

D. Microsoft Defender for DNS

Answer: B

Explanation:

www.atmicnetworks.com

.

Question: 136

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: A

Explanation:

Question: 137

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: A

Explanation:

www.atmicnetworks.com

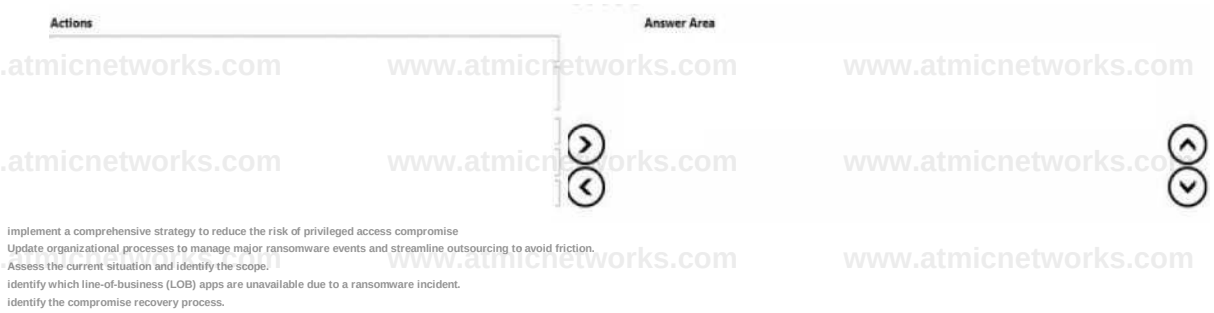
Question: 138

DRAG DROP

Your company wants to optimize ransomware incident investigations.

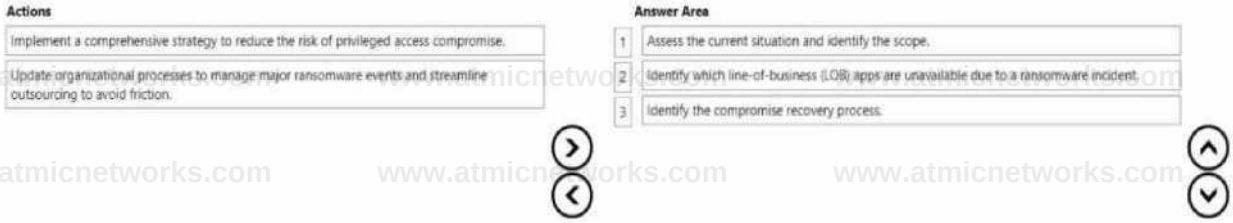
You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.

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.



Answer:

Explanation:



Question: 139

HOTSPOT

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

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

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

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

What should you use for each risk? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Are*

Deleted backups: Soft delete of backups *

(I3nS3ZTI3IZZ!3BBBIIMBII **Encryption by using a customer-managed key Multi-user authorization by using Resource Guard I 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

Soft delete of backups

Answer:

Explanation:

Answer Area

Deleted backups: Soft delete of backups

Disabled backups: Multi-user authorization by using Resource Guare

Question: 140

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

Explanation:

www.atmicnetworks.com

Question: 141

HOTSPOT

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.

Answwet Axe*

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

Custom entity activities

| A playbook

A threat detection rule

A threat indicator

A threat intelligence connector

Aulomaticalty generate incidents [A threat detevson rule

Custom entity activities

A playbook

A threat detection rule

A threat indicator

A threat intelligence connector

Answer:

Explanation:

Answer Area

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

Automatically generate incidents A threat detection rule

Question: 142

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

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

You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel.

What should you include m the recommendation?

A. an Azure logic app

B. an on-premises Syslog server

C. an on-premises data gateway

D. Azure Data Factory

Answer: B

Explanation:

Question: 143

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AO credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

A. an Azure AD enterprise application

B. a retying party trust in Active Directory Federation Services (AD FS)

C. Azure AD Application Proxy

D. Azure AD B2C

Answer: C

Explanation:

www.atmicnetworks.com

Question: 144

HOTSPOT

You have an Azure SQL database named DB1 that contains customer information.

A team of database administrators has full access to DB1.

To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information.

You need to design a security strategy for D81. The solution must meet the following requirements:

- When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.

When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.

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

NOTE: Each correct selection is worth one point.

Answer Area

For the database administrators: Always Encrypted

Dynamic data masking
Row-level security (RIS)
Transparent Data Encryption (TDE)

For the operators: Row-level security (RES)
Always Encrypted
Dynamic data masking

Transparent Data Encryption (TDE)

Explanation:

Answer Area

Answer:

For the database administrators: Always Encrypted

For the operators: Row-level security (RLS)

Question: 145

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: A, D

Explanation:

Question: 146

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

Explanation:

Question: 147

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to Appl.

What should you include in the design?

A. Azure AD Application Proxy

B. connected apps in Microsoft Defender for Cloud Apps

C. Microsoft Entra Identity Governance

D. access policies in Microsoft Defender for Cloud Apps

Answer: C

Explanation:

Question: 148

DRAG DROP

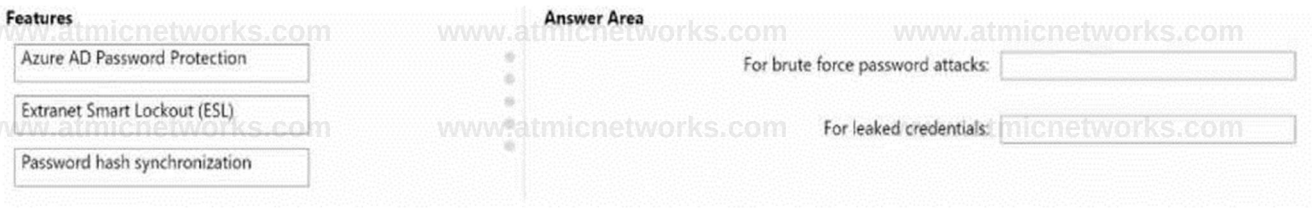
You have a hybrid Azure AD tenant that has pass-through authentication enabled.

You are designing an identity security strategy.

You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.

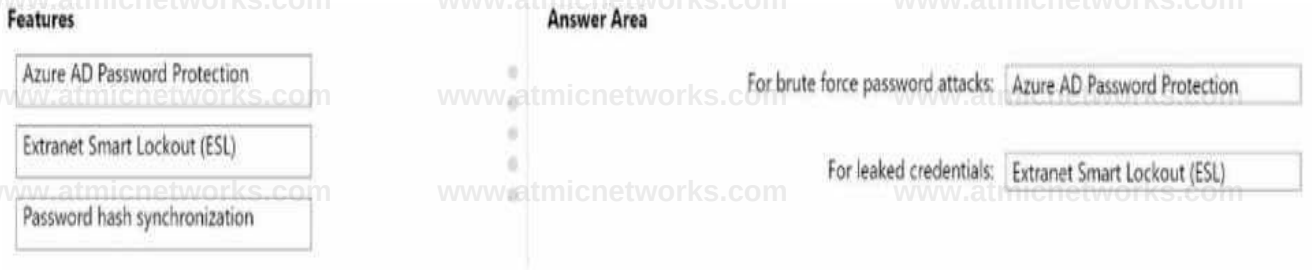
What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Explanation:

Answer:



Question: 149

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

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

Service:

- Microsoft Defender for Office 365
- Azure AD Identity Protection
- Microsoft Defender for DNS
- Microsoft Defender for Office 365
- Microsoft Purview

Policy type:

- Anti phishing
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

Explanation:

Answer:

Answer Area

Service: Microsoft Defender for Office 365

Policy type: Anti - phishing

Question: 150

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

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.

What should you include in the recommendation?

A. Microsoft Defender for Endpoint

B. Windows Defender Device Guard

C. protected folders

D. Azure Files

E. BitLocker Drive Encryption (BitLocker)

Answer: C

Explanation:

Question: 151

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

Explanation:

Question: 152

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

Explanation:

Question: 153

HOTSPOT

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.

Explanation:

Answer Area

Answer:

DLP: Microsoft Purview

UEBA: Azure AD Identity Protection

Question: 155

HOTSPOT

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

Answer:

Explanation:

Answer Area

Automatically identify threats: Microsoft Defender for Cloud

Enforce security settings: Microsoft Sentinel

Question: 156

HOTSPOT

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.

During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.

Threat modeling:

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

NOTE: Each correct selection is worth one point

Answer Area

Operate
Plan and develop

Dynamic application security testing (DASTI:

Build and test
Build and test
Commit the code
Go to production
Operate

Actionable intelligence:

Plan and develop
Build and test
Commit the code
Go to production

Answer:

Explanation:

Answer Area

Threat modeling: Plan and develop

Actionable intelligence: Operate

Dynamic application security testing (DAST): Build and test

Question: 157

You have legacy operational technology (OT) devices and IoT devices.

You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures (MCRA). The solution must minimize the risk of disrupting business operations.

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

NOTE: Each correct selection is worth one point

A. passive traffic monitoring

B. active scanning

C. threat monitoring

D. software patching

Answer: C, D

www.atmicnetworks.com

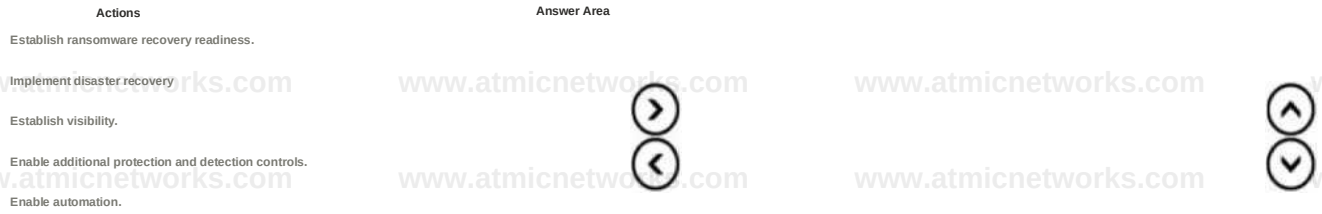
Question: 158

DRAG DROP

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

You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).

Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer, move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.



Answer:

Explanation:

Question: 159

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

Explanation:

Question: 160

HOTSPOT

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

FortheVDI:

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 foi Endpoint by using a custom Group Policy Object GPO)
Onboard the golden image to Defender for Endpoint.

Answer:

Explanation:

Answer Area

For the VEN: Add the Defender for Endpoint onboarding script to the virtual machine template.

For Azure Virtual Desktop Add the Defender for Endpoint onboarding script to the golden image.

Question: 161

HOTSPOT

Your company, named Contoso. Ltd... has an Azure AD tenant namedcontoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:

- Follow the principle of least privilege.
- Minimize administrative effort.

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

Answer Area

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

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

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

Answer:

Explanation:

Answer Area

Role to assign to the Fabrikam helpdesk users for conloso.com: Password Administrator

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

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

Question: 162

HOTSPOT

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
| Azure Automation
Azure Bastion
| Just-in-time (JIT) VM access

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

Answer:

Explanation:

Answer Area

Manage NSG rules by using: Azure Bastion

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

Question: 163

HOTSPOT

You plan to automate the development and deployment of a Nodejs-based app by using GitHub.

You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

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

What should you recommend using? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To automate vulnerability code scanning; | GitHub Enterprise Cloud T |

GitHub Enterprise Cloud

GitHub Enterprise Server

GitHub Team

To automatically generate pull requests. I Deoendabot | Codespaces

Dependabot

| Dependency Tracker

Answer:

Explanation:

Answer Area

To automate vulnerability code scanning: GitHub Enterprise Cloud

To automatically generate puli requests: Dependabot

Question: 164

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

Explanation:

Question: 165

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.

www.atmicnetworks.com

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 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 Microsoft-managed keys.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 166

You have an Azure AD tenant that contains 10 Windows 11 devices and two groups named Group1 and Group2. The Windows 11 devices are joined to the Azure AD tenant and are managed by using Microsoft Intune.

You are designing a privileged access strategy based on the rapid modernization plan (RaMP). The strategy will include the following configurations:

- Each user in Group1 will be assigned a Windows 11 device that will be configured as a privileged access device.
- The Security Administrator role will be mapped to the privileged access security level.
- The users in Group1 will be assigned the Security Administrator role.
- The users in Group2 will manage the privileged access devices.

You need to configure the local Administrators group for each privileged access device. The solution must follow the principle of least privilege.

What should you include in the solution?

A. Only add Group2 to the local Administrators group.

B. Configure Windows Local Administrator Password Solution (Windows LAPS) in legacy Microsoft LAPS emulation mode.

C. Add Group2 to the local Administrators group. Add the user that is assigned the Security Administrator role to the local Administrators group of the user's assigned privileged access device.

Answer: B

Explanation:

Question: 167

You have a Microsoft 365 subscription. You have an Azure subscription.

You need to implement a Microsoft Purview communication compliance solution for Microsoft Teams and Yammer. The solution must meet the following requirements:

- Assign compliance policies to Microsoft 365 groups based on custom Microsoft Exchange Online attributes.
- Minimize the number of compliance policies
- Minimize administrative effort

What should you include in the solution?

A. Azure AD Information Protection labels

B. Microsoft 365 Defender user tags

C. adaptive scopes

D. administrative units

Answer: C

Explanation:

Question: 168

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You need to enforce ISO 27001:2013 standards for new resources deployed to the subscription. The solution must ensure that noncompliant resources are automatically detected.

What should you use?

A. Azure Blueprints

B. the regulatory compliance dashboard in Defender for Cloud

C. Azure role-based access control (Azure RBAC)

D. Azure Policy

Answer: D

Explanation:

Question: 169

HOTSPOT

You have an Azure subscription that contains a Microsoft Sentinel workspace named MSW1. MSW1 includes 50 scheduled analytics rules.

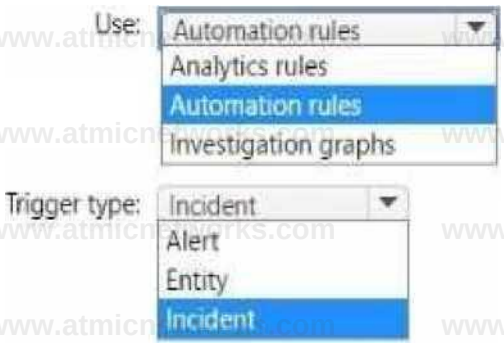
You need to design a security orchestration automated response (SOAR) solution by using Microsoft Sentinel playbooks. The solution must meet the following requirements:

- Ensure that expiration dates can be configured when a playbook runs.
- Minimize the administrative effort required to configure individual analytics rules.

What should you use to invoke the playbooks, and which type of Microsoft Sentinel trigger should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Use: Automation rules

Trigger type: Incident

www.atmicnetworks.com

Question: 170

HOTSPOT

You have an Azure subscription. The subscription contains an Azure application gateway that use Azure Web Application Firewall (WAF).

You deploy new Azure App Services web apps. Each app is registered automatically in the DNS domain of your company and accessible from the Internet.

You need to recommend a security solution that meets the following requirements:

- Detects vulnerability scans of the apps
- Detects whether newly deployed apps are vulnerable to attack

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

Answer Area

To detect vulnerability scans of the apps

Microsoft Defender for ADD Service
Azure WAF
Microsoft Defender External Attack Surface Management (Defender EASM)
Microsoft Defender for App Service
Microsoft Defender for Cloud ADDS

To detect whether newly deployed apps are vulnerable to attack

Microsoft Defender for ADD Service
Azure WAF
Microsoft Defender External Attack Surface Management (Defender EASM)
Microsoft Defender for App Service
Microsoft Defender for Cloud Apps

Answer:

Explanation:

Answer Area

To detect vulnerability scans of the apps Microsoft Defender for App Service

To detect whether newly deployed apps are vulnerable to attack Microsoft Defender for App Service

Question: 171

You have an on-premises server that runs Windows Server and contains a Microsoft SQL Server database named DB1.

You plan to migrate DB1 to Azure.

You need to recommend an encrypted Azure database solution that meets the following requirements:

- Minimizes the risks of malware that uses elevated privileges to access sensitive data

- Prevents database administrators from accessing sensitive data
- Enables pattern matching for server-side database operations
- Supports Microsoft Azure Attestation
- Uses hardware-based encryption

What should you include in the recommendation?

A. SQL Server on Azure Virtual Machines with virtualization-based security (VBS) enclaves

B. Azure SQL Database with virtualization-based security (VBS) enclaves

C. Azure SQL Managed Instance that has Always Encrypted configured

D. Azure SQL Database with Intel Software Guard Extensions (Intel SGX) enclaves

Answer: D

Explanation:

Question: 172

You plan to deploy 20 Azure Kubernetes Service (AKS) clusters. The cluster configuration will be managed declaratively by using Kubernetes manifest files stored in Azure Repos.

You need to recommend a solution to ensure that the configuration of all the clusters remains consistent by using the manifest files stored in Azure Repos.

What should you include in the recommendation?

A. Gatekeeper

B. Dependency Tracker

C. Dependency

D. Flux

Answer: D

Explanation:

www.atmicnetworks.com

Question: 173

You have a Microsoft 365 tenant that contains 5,000 users and 5,000 Windows 11 devices. All users are assigned Microsoft 365 £5 licenses and the Microsoft Defender Vulnerability Management addon. The Windows 11 devices are managed by using Microsoft Intune and Microsoft Defender for Endpoint. The Windows 11 devices are configured during deployment to comply with Center for Internet Security (CIS) benchmarks for Windows 11.

You need to recommend a compliance solution for the Windows 11 devices. The solution must identify devices that were modified and no longer comply with the CIS benchmarks.

What should you include in the recommendation?

A. Authenticated scan for Windows in Microsoft Defender Vulnerability Management

B. Microsoft Secure Score for Devices in Defender for Endpoint

C. attack surface reduction (ASR) rules in Defender for Endpoint

D. security baselines assessments in Microsoft Defender Vulnerability Management

Answer: D

Explanation:

Question: 174

HOTSPOT

You have a Microsoft 365 tenant.

You need to recommend a Microsoft 365 Defender solution to enhance security for the tenant. The solution must meet the following requirements:

- Identify users that are downloading an unusually high number of files from Microsoft SharePoint Online sites and are possibly involved in a data exfiltration attempt.
- Block Microsoft Teams messages that contain potentially malicious content by using zero-hour auto purge (ZAP).

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

identify data exfiltration attempts' Microsoft Defender for Cloud Apps

Microsoft Defender for Endpoint
Microsoft Defender for identity
Microsoft Defender for Office 365

Block Teams messages: Microsoft Defender fot Office 365

Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Defender for Identity

Answer

Explanation:

Answer Area

identify data exfiltration attempts: Microsoft Defender for Cloud Apps

Block Teams messages: Microsoft Defender for Office 365

Question: 175

HOTSPOT

You have three Microsoft Entra tenants named Tenant 1. Tenant2. and Tenant3.

You have three Azure subscriptions named Sub1, Sub2, and Sub3. Each tenant is associated with multiple Azure subscriptions.

Each subscription contains a single Microsoft Sentinel workspace as shown in the following table.

Name	Subscription	Associated tenant
Sentinel1	Sub1	Tenant1
Sentinel2	Sub2	Tenant2
Sentinel3	Sub3	Tenant3

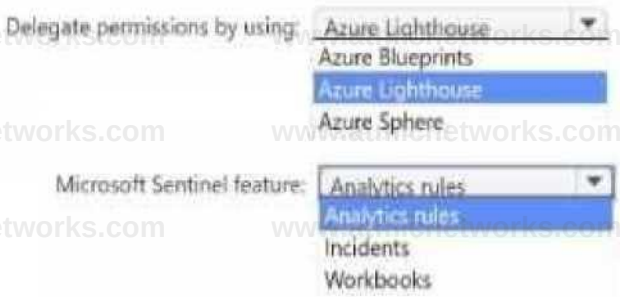
You need to recommend a solution that meets the following requirements:

- Ensures that the users in Tenant1 can manage the resources in Sub2 and Sub3 without having to switch subscriptions or sign in to a different tenant
- Implements multiple workspace view for Sentinel2 and Sentinel3

What should you use to delegate permissions, and which Microsoft Sentinel feature will users be able to manage in multiple workspace view? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Delegate permissions by using Azure Lighthouse

Microsoft Sentinel feature: Analytics rules

Question: 176

You have an Azure subscription

You plan to deploy multiple containerized microservice-based apps to Azure Kubemetes Service (AKS)

You need to recommend a solution that meets the following requirements:

- Manages secrets
- Provides encryption
- Secures service-to-service communication by using mTLS encryption
- Minimizes administrative effort

What should you include in the recommendation?

A. Flux

B. Envoy

C. Dapr

D. Istio

Answer: D

Explanation:

Question: 177

You have a multicloud environment that contains Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) subscriptions.

You need to discover and review role assignments across the subscriptions.

What should you use?

A. Microsoft Entra Permissions Management

B. Microsoft Defender for Identity

C. Azure Lighthouse

D. Microsoft Entra ID Governance

Explanation:

Answer: C

Question: 178

HOTSPOT

You have an Azure subscription.

You plan to implement Azure Synapse Analytics SQL dedicated pools and SQL serverless pools.

You need to recommend a solution to provide additional encryption-at-rest security for each type of pool.

The solution must use customer-managed keys, whenever possible.

What should you recommend for each pool type? To answer, drag the appropriate recommendations to the correct pool types. Each recommendation 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.

Answer Area

Serverless SQL pool

Azure Storage infrastructure encryption aneHMicrosoft -managed keys

Transparent Data Encryption (TDE) and customer-managed keys Transparent Data Encryption (TDE) and Microsoft-managed keys

Dedicated SQL pool

u'vocr- -.ra Encrypti:-' ;_L; an;: c^tzra ^jrjccc kc,:

Azure Storage infrastructure encryption and Microsoft-managed keys

Transparent Data Encryption (IDE) and customer managed keys 1

Transparent Data Encryption (TDE) and Microsoft-managed keys

Answer:

Explanation:

Answer Area

Serverless SQL pool Azure Storage infrastructure encryption and Microsoft-managed keys

Dedicated SQL pool: Transparent Data Encryption i^)E) and customer-managed keys

Question: 179

You have an on-premises app named App1. Remote users access App1 by using VPN connections.

You have a third-party software as a service (SaaS) app named App2. You need to deploy Global Secure Access to manage access to App1 and App2. What should you use for each app?

A. Microsoft Entra Private Access for App1 and Microsoft Entra Internet Access for App2

B. Microsoft Entra Private Access for App1 and App2

C. Microsoft Entra Internet Access for App1 and App2

D. Microsoft Entra Private Access for App2 and Microsoft Entra Internet Access for App1

Answer: A

Explanation:

Question: 180

You have an Azure subscription that contains multiple network security groups (NSGs), multiple virtual machines, and an Azure Bastion host named bastion1.

Several NSGs contain rules that allow direct RDP access to the virtual machines by bypassing bastion

You need to ensure that the virtual machines can be accessed only by using bastion! The solution must prevent the use of NSG rules to bypass bastion1.

What should you include in the solution?

A. Azure Virtual Network Manager connectivity configurations

B. Azure Virtual Network Manager security admin rules

C. Azure Firewall application rules

D. Azure Firewall network rules

Answer: B

Explanation:

Question: 181

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to deploy Global Secure Access universal tenant restrictions v2.

Which authentication plane resources and which data plane resources will be protected? To answer, select the appropriate options in the answer area.

All Miciosoft Entra ID integrated apps, fciuding third-party apps
All Microsoft Entra ID integrated apps^iduding third-party apps
All Microsoft 365 apps
Microsoft SharePoint Online and Exchange Online only

NOTE: Each correct selection is worth one point.

Answer Area

Authentication plane resources:

Microsoft SharePoint Online and Exchange Online only

Data plane resources:

All Microsoft 365 apps

All Microsoft Entra ID integrated apps. including third-party apps
All Microsoft 365 apps

Answer:

Explanation:

Answer Area

Authentication plane resources All Microsoft Entra ID integrated apps, including third-party apps

Data plane resources: All Microsoft 365 apps

Question: 182

Your company has a main office and 10 branch offices. Each branch office contains an on-premises file server that runs Windows Server and multiple devices that run either Windows 11 or macOS. The devices are enrolled in Microsoft Intune.

You have a Microsoft Entra tenant.

You need to deploy Global Secure Access to implement web filtering for device traffic to the internet The solution must ensure that all the web traffic from the devices in the branch offices is controlled by using Global Secure Access.

What should you do first in each branch office?

A. Configure an Intune policy to deploy the Global Secure Access client to each device.

B. Configure an IPsec tunnel on the router.

C. Install the Microsoft Entra private network connector on the file server.

D. Configure an Intune policy to onboard Microsoft Defender for Endpoint to each device.

Answer: B

Explanation:

Question: 183

You have an Azure Kubernetes Service (AKS) cluster that hosts Linux nodes.

You need to recommend a solution to ensure that deployed worker nodes have the latest kernel updates. The solution must minimize administrative effort.

What should you recommend?

A. The AKS cluster version must be upgraded.

B. The updates must first be applied to the image used to provision the nodes.

C. The nodes must restart after the updates are applied.

Answer: B

Explanation:

Question: 184

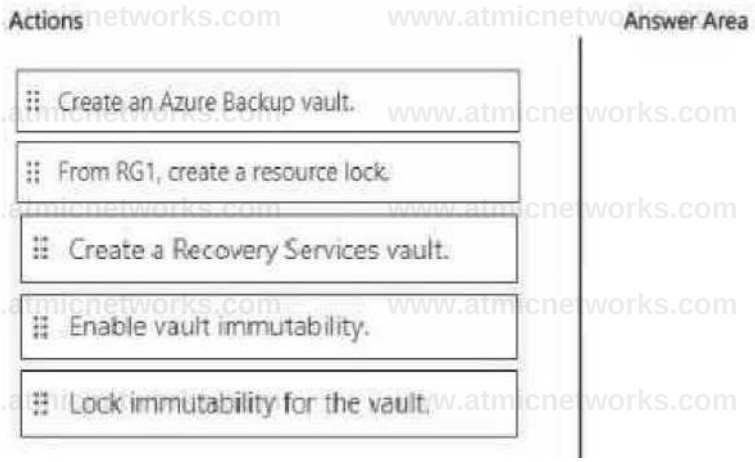
DRAG DROP

You have an Azure subscription that contains a resources group named RG1. RG1 contains multiple Azure Files shares.

You need to recommend a solution to deploy a backup solution for the shares. The solution must meet the following requirements:

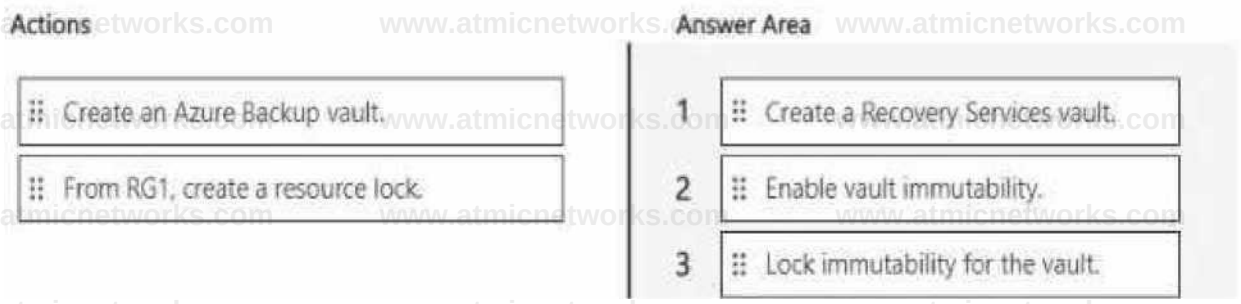
- Prevent the deletion of backups and the vault used to store the backups.
- Prevent privilege escalation attacks against the backup solution.
- Prevent the modification of the backup retention period.

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



Answer:

Explanation:



Question: 185

HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNet!	Virtual network	Contains two subnets named Subnet 1 and Subnet?
VM1	Virtual machine	Runs an app named Appl and is connected to Subnetl
DB1	Azure SQL Database	Contains data for App 1 and is accessible from the internet

You need to recommend a network security solution for App1. The solution must meet the following requirements:

- Only the virtual machines that are connected to Subnet1 must be able to connect to D81.
- DB1 must be inaccessible from the internet
- Costs must be minimized.
- What should you include in the recommendation? To answer, select the options in the answer area.
- NOTE: Each correct answer is worth one point.

Answer Area

io ensure that only VM1 can access DB1

A private endpoint

A private endpoint

Azure Application Gateway

Azure Private Link

To enforce network security restrictions for DB1:

Network security groups (NSGs)

| Azure Firewall rules

Network security groups (NSGs)

| Virtual network rules

Answer:

Explanation:

Answer Area

10 ensure that only VM1 can access DB1: A private endpoint

To enforce network security restrictions for DB1: Network security groups INSGs)

Question: 186

HOTSPOT

You have an Azure subscription.

You plan to deploy a storage account named storage1 that will store confidential data. You will assign tags to the confidential data.

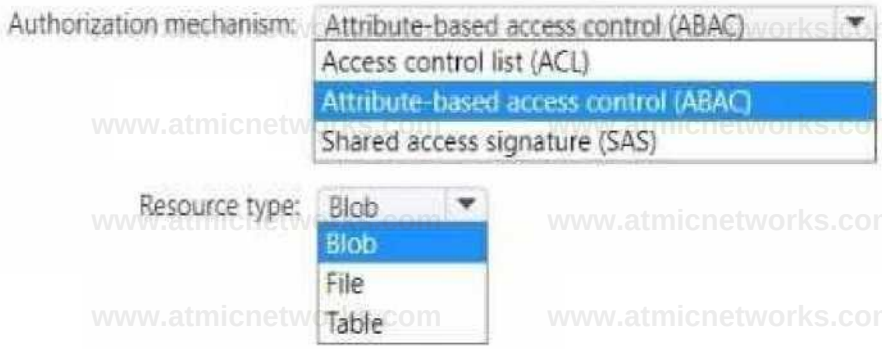
You need to ensure that access to storage1 can be defined by using the assigned tags.

Which authorization mechanism should you enable, and which type of resource should you use to store the data? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

www.atmicnetworks.com

Answer Area



Answer:

Explanation:

Answer Area

Authorization mechanism: Attribute-based access control (ABAC)

Resource type: Blob

Question: 187

HOTSPOT

Your company has offices in New York City and Los Angeles.

The New York City office contains an on-premises app named Appl.

You have an Azure subscription. The subscription is linked to a Microsoft Entra tenant that is hosted in North America.

You plan to manage access to App1 for the users in the Los Angeles office by using Microsoft Entra Private Access.

You will deploy Private Access by performing the following actions:

- Provision an ExpressRoute circuit from the New York City office to the closest peering location.
- Create an Azure virtual network named VNet1 in the East US Azure region.
- Deploy a Microsoft Entra application proxy connector to VNet1.

You need to optimize the network for the planned deployment The solution must meet the following requirements:

- Maximize redundancy for connectivity to App1.
- Minimize network latency when accessing App1
- Minimize complexity.
- Minimize costs.

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

To optimize the connection between the users and the appl icanon Two connectors to the default connector group proxy, deploy: IA connector to the default connector group and a connector to a new connector group

Iwo connectors to the default connector group

(Two new connector groups that each contain a new connector

To optimize the connection between the connector and App1, use ExpressRoute with Microsoft peering

ExpressRoute with Microsoft peering

ExpressRoute with Microsoft peering and the premium add-on
ExpressRoute with private peering

Answer Explanation:

Answer Area

To optimize the connection between the users and the application proxy, deploy:

Two connectors to the default connector group

To optimize the connection between the connector and Appt, use:

ExpressRoute with Microsoft peering

Question: 188

HOTSPOT

You have an Azure subscription that contains multiple apps. The apps are managed by using continuous integration and continuous deployment (CI/CD) pipelines in Azure DevOps.

You need to recommend DevSecOps controls for the Commit the code and the Build and test CI/CD process stages based on the Microsoft Cloud Adoption Framework for Azure.

Which testing method should you recommend for each stage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Commit the code: Static application security testing (SAST)

Dynamic application security testing (DAST)
Penetration testing
Smoke testing
Static application security testing (SAST)

Build and test: Dynamic application security testing (PAST)

Dynamic application security testing (DAST)
Penetration testing
Smoke testing
Static application security testing (SAST)

Explanation:

Answer:

Answer Area

Commit the code: Static application security testing (SAST)

Build and test; | Dynamic application security testing |DASI[

www.atmicnetworks.com

Question: 189

You have a Microsoft 365 subscription that contains 1,000 users. Each user is assigned a Microsoft 365 E5 license.

The subscription uses sensitivity labels to classify corporate documents. All the users have Windows 11 devices that are onboarded to Microsoft Defender for Endpoint and are configured to sync files to Microsoft OneDrive.

You need to prevent the users from uploading the documents from OneDrive to external websites.

What should you include in the solution?

A. Microsoft Purview Information Protection

B. Microsoft Purview data loss prevention (DLP)

C. web content filtering in Defender for Endpoint

D. an endpoint security policy

Answer: B

Explanation:

Question: 190

HOTSPOT

You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1.

You need to configure WS1 to meet the following requirements:

- Create custom dashboards to visualize the workload of security analysts that use Microsoft Sentinel.
- Enable automated responses for the security alerts generated by Microsoft Sentinel analytics rules.

What should you use for each requirement? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Custom dashboards: Workbooks Notebooks

Playbooks

Workbooks

Automated responses: Playbooks

| Notebooks
Playbooks
| Workbooks

Answer:

Explanation:

Answer Area

Custom dashboards: Workbooks

Automated responses: Playbooks

Question: 191

HOTSPOT

You have a Microsoft 365 subscription that contains 1,000 users and two groups named Group1 and Group2. All the users have devices that are onboarded to Microsoft Intune and Microsoft Defender for Endpoint Group1 manages Microsoft Entra and Microsoft 365 services. Group2 manages Intune and Defender for Endpoint.

You need to recommend a solution to prevent users from connecting to Microsoft 365 services from devices that have encryption disabled.

What should you recommend implementing for each group? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Groupl. | A Conditional Access policy T |

A Conditional Access policy

A sign-in risk policy in Microsoft Entra ID Protection A user risk policy in Microsoft Entra ID Protection Microsoft Defender for Office 365

Group2: A compliance policy in Intune

A compliance policy in Intune

A configuration profile in Intune

A Defender for Endpoint attack surface reduction (ASR) rule An endpoint security policy

Answer:

Explanation:

Answer Area

Grou p 1: A Conditional Access policy

Group2: A compliance policy in Intune

Question: 192

You have an Azure subscription that contains multiple Azure Data Lake Storage accounts.

You need to recommend a solution to encrypt the content of the accounts by using service-side encryption and customer-managed keys. The solution must ensure that individual encryption keys are applied at the most granular level.

At which level should you recommend the encryption be applied?

A. account

B. folder

C. file

D. container

Answer: D

www.atmicnetworks.com

Question: 193

HOTSPOT

You are designing a privileged access strategy for a company named Contoso, Ltd. and its partner company named Fabrikam, Inc. Contoso has a Microsoft Entra tenant named contoso.com. Fabrikam has a Microsoft Entra tenant named fabrikam.com. Users at Fabrikam must access the resources in contoso.com.

You need to provide the Fabrikam users with access to the Contoso resources by using access packages. The solution must meet the following requirements:

- Ensure that the Fabrikam users can use the Contoso access packages without explicitly creating guest accounts in contoso.com.
- Allow non-administrative users in contoso.com to create the access packages.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Ensure that the Fabrikam users can use the access packages Without explicitly creating guest accounts in contoso.com

A connected organization

A connected organization
An external organization
An identity provider

Allow nan-administrative users in contoso com to create the access packages by creating:

Catalogs

Administrative units
Catalogs
Programs

Answer:

Explanation:

Answer Area

Ensure that the Fabrikam users can use the access packages without explicitly creating guest accounts in contoso.com

A connected organization

Allow non-administrative users in contoso com to create the access packages

Catalogs

Question: 194

You have to Azure subscriptions that contain 100 role-based access control (RBAC) role assignments. You plan to consolidate the role assignments.

You need to recommend a solution to identify which role assignments were NOT used during the last 90 days. The solution must minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Defender for Cloud

B. Microsoft Entra access reviews

C. Microsoft Entra Privileged Identity Management (PIM)

D. Microsoft Entra Permissions Management

Answer: D

Explanation:

Question: 195

HOTSPOT

You have an Azure subscription that contains 100 virtual machines. The virtual machines are accessed by using Azure Bastion.

You need to recommend a solution to ensure that only specific users in specific locations can access the virtual machines. The solution must meet the following requirements:

- Restrict access to the virtual machines based on an originating IP address or a connection request by using just-in-time (JIT) VM access network-based controls.
- Restrict access to the virtual machines based on role-based access control (RBAC) role assignments by using JIT VM access authorization controls.

Which Microsoft cloud services should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

For the network controls: Microsoft Defender for Cloud ”

For the authorization controls: Microsoft Entra Privileged Identity Management (PIM)

Question: 196

You have a Microsoft 365 tenant that uses Microsoft SharePoint Online and Microsoft Purview. Microsoft Purview has a sensitivity label named Label1 that is applied to the files stored on SharePoint Online sites.

You need to recommend a Microsoft Purview Data Loss Prevention (DLP) policy that meets the following requirements:

- Prevents users from uploading the files to third-party external websites
- Allows users to upload the files to Microsoft OneDrive for Business

To which location should you apply the DLP policy?

A. Devices

B. OneDrive accounts

C. SharePoint sites

D. Microsoft Defender for Cloud Apps

Answer: A

Explanation:

Question: 197

Your on-premises network contains an Active Directory Domain Services (AD DS) domain named corpxontoso.com and an AD DS-integrated application named App1.

Your perimeter network contains a server named Server1 that runs Windows Server.

You have a Microsoft Entra tenant named contoso.com that syncs with corp.contoso.com.

You plan to implement a security solution that will include the following configurations:

- Manage access to App1 by using Microsoft Entra Private Access.
- Deploy a Microsoft Entra application proxy connector to Server1.
- Implement single sign-on (SSO) for App1 by using Kerberos constrained delegation.
- For Server1, configure the following rules in Windows Defender Firewall with Advanced Security:

o Rule1: Allow TCP 443 inbound from a designated set of Azure URLs.

o Rule2: Allow TCP 443 outbound to a designated set of Azure URLs.

o Rule3: Allow TCP 80 outbound to a designated set of Azure URLs.

o Rule4: Allow TCP 389 outbound to the domain controllers on corp.contoso.com.

You need to maximize security for the planned implementation. The solution must minimize the impact on the connector.

Which rule should you remove?

A. Rule1

B. Rule2

C. Rule3

D. Rule4

Answer: C

Explanation:

Question: 198

You have a Microsoft Entra tenant. The tenant contains 500 Windows devices that have the Global Secure Access client deployed.

You have a third-party software as a service (SaaS) app named App1.

You plan to implement Global Secure Access to manage access to App1.

You need to recommend a solution to manage connections to App1. The solution must ensure that users authenticate by using their Microsoft Entra credentials before they can connect to App1.

What should you include the recommendation?

A. a Global Secure Access app

B. a private access traffic forwarding profile

C. an internet access traffic forwarding profile

D. a Quick Access app

Answer: A

Explanation:

www.atmicnetworks.com

Question: 199

You have a Microsoft Entra tenant named contoso.com and use Microsoft Intune. Each user in contoso.com has a Microsoft Entra ID P1 license and a Windows 11 device that has the Global Secure Access client deployed.

You plan to deploy the following configuration of Microsoft Entra Internet Access:

- Enable a baseline profile.
- Create a security profile named Profile` that has a priority of 300 and contains a single web content filtering policy named WCFPolicy configure WCFPolicy1 as follows:
  - o Set Action to allow.
  - o Include a single rule that has a fully qualified domain name (FQDN) destination of '. adatum.com.
- Link Profile1 to a Conditional Access policy named CAPolicy1, apply CAPolicy1 to all users, and grant access unless a user's device is noncompliant

You need to evaluate the impact of the planned deployment on traffic to the following resources:

- https://www.adatum.com:8433
- https://www.fabrikam.com

Which two traffic scenarios will occur? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point

A. Traffic to https://www.fabrikam.com will be allowed from all the devices.

B. Traffic to https://www.adatum.com:8433 will be blocked from all the devices.

C. Traffic to https://www.adatumxom:8433 will be allowed from all the devices.

D. Traffic to https://www.fabrikam.com will be allowed from compliant devices only.

E. Traffic to https://www.adatum.com:8433 will be allowed from compliant devices only.

F. Traffic to https://www.fabrikam.com will be blocked from noncompliant devices only.

Answer: A, E

Explanation:

Question: 200

You have a multicloud environment that contains an Azure subscription, an Amazon Web Services (AWS) subscription, and a Google Cloud Platform (GCP) subscription.

You plan to assess data security and compliance.

You need to design a Compliance Manager solution that meets the following requirements:

- Provides recommended improvement actions that include detailed implementation guidance
- Automatically monitors regulatory compliance
- Minimizes administrative effort

What should you include in the solution?

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

Answer: A

Explanation:

Question: 201

You have two Azure subscriptions named Sub1 and Sub2 that contain the vaults shown in the following table.

Name	Type	Location	Subscription
RSVault1	Recovery Services vault	East US	Sub1
BackupVault1	Azure Backup vault	East US	Sub2
RSVault2	Recovery Services vault	West US	Sub2
BackupVault2	Azure Backup vault	West US	Sub1

You need to design a multi-user authorization (MUA) solution for security operations on the vaults.

The solution must meet the following requirements:

- RSVault1 and RSVault2 must require MUA for disabling soft delete, removing MUA protection, and disabling immutability.
- BackupVault1 and BackupVault2 must require MUA for disabling soft delete and removing MUA protection.

What is the minimum number of Resource Guard resources required?

A. 1
B. 2
C. 3
D. 4

Answer: C

Explanation:

Question: 202

You have an Azure subscription and an Azure DevOps organization.

You need to recommend a solution for connecting Azure DevOps pipelines to the resources in the subscription by using Azure Resource Manager (ARM) service connections. The solution must align with Microsoft Cloud Adoption Framework for Azure best practices, including the principle of least privilege.

What should you include in the recommendation?

A. workload identity federation and system-assigned managed identities
B. service principals and secrets
C. workload identity federation and user-assigned managed identities
D. workload identity federation and service principals

Answer: C

Explanation:

Question: 203

HOTSPOT

You have an Azure DevOps organization that is used to manage the development and deployment of internal apps to multiple Azure subscriptions.

You need to implement a DevSecOps strategy based on Microsoft Cloud Adoption Framework for Azure principles. The solution must meet the following requirements:

- All pull requests must be enforced.
- All deployments to production must be approved.

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

All pull requests must be enforced: Protected branches

Environments
Protected branches
Resource locks

All deployments to production must be approved: Environments

Environments
Resource locks
Triggers

Answer:

Explanation:

Answer Area

All pull requests must be enforced: Protected branches

All deployments to production must be approved: Environments

Question: 204

You have multiple Azure subscriptions that each contains multiple resource groups.

You need to identify the privileged role assignments in each subscription and any associated security risks. The solution must minimize administrative effort.

What should you use?

A. The Analytics dashboard in Microsoft Entra Permissions Management
B. access reviews in Microsoft Entra ID Identity Governance
C. access reviews in Privileged Identity Management (PIM)
D. Microsoft Defender External Attack Surface Management (Defender EASM) discovery

Answer: C

Explanation:

www.atmicnetworks.com

Question: 205

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a hybrid deployment between a Microsoft Exchange Server 2019 organization and an Exchange Online tenant. The AD DS domain contains a group named Group1. Group1 is a member of the Organization Management role group for the Exchange deployment.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender.

You have an Azure subscription that uses Microsoft Sentinel.

You need to recommend a solution to ensure that Group1 is marked as a sensitive group and that any changes made to Group1 raises an alert in Microsoft Sentinel. The solution must minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Entra ID Protection
B. Microsoft Defender for Identity
C. Microsoft Defender for Office 365
D. Microsoft Entra Privileged Identity Management (PIM)

Answer: B

Explanation:

Question: 206

HOTSPOT

You have an Azure subscription that contains multiple storage accounts. The accounts contain Azure Files shares and Azure Blob Storage containers. The accounts have encryption scopes and infrastructure encryption enabled.

You need to implement customer-managed key-based encryption for the shares and the containers. The solution must ensure that the encryption keys are applied at the most granular level.

At which level should you apply the encryption keys? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

For the containers: Blob

For the shares: Account

Question: 207

HOTSPOT

You have the Azure subscriptions shown in the following table.

Name	Linked Microsoft Entra tenant	Description
Sub1	contoso.com	Contains an Azure Backup vault named Vaultl
Sub2	contososecurity.com	Used to manage secunty resources

The tenants contain the groups shown in the following table.

Name	Tenant	Members
Group 1	contoso.com	Administrators who manage Azure Backup for Sub1
Group?	contososecurity com	Administrators who manage security for Sub1 and Sub2

You perform the following actions:

- Configure multi-user authorization (MUA) for Vault1 by using a resource guard deployed to Sub2.
- Enable all available MUA controls for Vault1.
- In contoso.com, create a Privileged Identity Management (PIM) assignment named Assignment1.
- Configure Assignment1 to enable Group! to activate the Contributor role for Vault1.

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
To enable MUA for Vaultl, a resource guard must be deployed to Sub1		
A user in Group2 must approve changes made by a user in Group! to the backup policies of Vaultl.	O	O
A user in Groupl that activates Assignmentl can disable soft delete for the backups of Vaultl, without the approval of a user in Group2,	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
To enable MUA for Vaultl, a resource guard must be deployed to Sub1.	O	®
A user in Group2 must approve changes made by a user in Group! to the backup policies of Vault!.	®	O
A user in Group! that activates Assignment! can disable soft delete for the backups of Vault!, without the approval of a user in Group2	O	®

Question: 208

You have an Azure subscription.

You plan to deploy enterprise-scale landing zones based on the Microsoft Cloud Adoption Framework for Azure. The deployment will include a single-platform landing zone for all shared services and three application landing zones that will each host a different Azure application.

You need to recommend which resource to deploy to each landing zone. The solution must meet the Cloud

Adoption Framework best-practice recommendations for enterprise-scale landing zones.
What should you recommend?

A. an Azure Private DNS zone
B. an Azure key vault
C. an Azure firewall
D. an Azure virtual network gateway

Answer: A

Explanation:

Question: 209

You have an Azure subscription.
You plan to deploy Azure Kubernetes Service (AKS) clusters that will be used to host web services.
You need to recommend an ingress controller solution that will protect the hosted web services.
What should you include in the recommendation?

A. Azure Load Balancer
B. Azure Front Door
C. Azure Firewall
D. Azure Application Gateway

Answer: D

Explanation:

Question: 210

You have an Azure subscription.
You plan to deploy Azure App Services apps by using Azure DevOps.
You need to recommend a solution to ensure that deployed apps maintain compliance with Microsoft cloud security benchmark (MCSB) recommendations.
What should you include in the recommendation?

A. DevOps security in Microsoft Defender for Cloud
B. Microsoft Defender for App Service
C. a branch policy in Azure DevOps
D. Azure Policy

Answer: D

Explanation:

Question: 211

You have an on-premises datacenter and an Azure Kubernetes Service (AKS) cluster named AKS1. You need to restrict internet access to the public endpoint of AKS 1. The solution must ensure that AKS1 can be accessed only from the public IP addresses associated with the on-premises datacenter. What should you use?

A. a network security group (N5G)
B. a service endpoint
C. a private endpoint
D. an authorized IP range

Answer: D

Explanation:

Question: 212

HOTSPOT

Your company has two offices named Office1 and Office2. The offices contain 1,000 on-premises Windows 11 devices that are Microsoft Entra joined.

You have a Microsoft 365 subscription and use Microsoft Intune.
You plan to deploy Microsoft Entra Internet Access from the offices to Microsoft 365.
You enable the Microsoft 365 profile and configure the following:

- A traffic policy for all Microsoft 365 traffic
- A linked Conditional Access policy that has the following configurations:
  ° Applies to all users
  ° Performs compliant network checks
  o Allows Microsoft 365 traffic from compliant devices
- An assignment to all devices
- An assignment to the remote network associated with Office1

You deploy the Global Secure Access client to all the devices in Office2 and establish connections.
Which users can access Microsoft 365 services from compliant devices, and which users are blocket1 from accessing Microsoft 365 services when using noncompliar devices? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Compliant devices: office 1 and Office2
Office! only
Office2 only
Office! and Office2

Noncompliant devices: Office! only
Office1 only
Office2 only
Office1 and Office2

Answer:

Explanation:

Answer Area

Compliant devices: Office! and Office?

Noncompliant devices: Office! only

www.atmicnetworks.com

Question: 213

You have an Azure subscription that contains 100 virtual machines, a virtual network named VNet1, and 20 users. The virtual machines run Windows Server and are connected to VNet1. The users work remotely and access Azure resources from Linux workstations.

You need to ensure that the users can connect to the virtual machines from the workstations by using Secure Shell {SSH). The solution must meet the following requirements:

- Ensure that the users authenticate by using their Microsoft Entra credentials.
- Prevent the users from transferring files from the virtual machines by using SSH.
- Prevent the users from directly accessing the virtual machines by using the public IP address of the virtual machines.

What should you include in the solution?

A. Azure Bastion
B. Azure NAT Gateway
C. just-in-time (JIT) VM access
D. Point-to-Site (P2S) VPN

Answer: A

Explanation:

Question: 214

You have a Microsoft 365 tenant named contoso.com.

You need to ensure that users can authenticate only to contoso.com. The solution must meet the following requirements:

- Prevent the users from authenticating to other Microsoft 365 tenants.
- Minimize administrative effort.

What should you use?

A. Microsoft Defender for Endpoint
B. Microsoft Entra Internet Access
C. Microsoft Entra Private Access
D. Microsoft Defender for Cloud Apps

Answer: C

Explanation:

Question: 215

You have on-premises Windows 11 devices that have the Global Secure Access client deployed.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online and Exchange Online.

You deploy Microsoft Entra Internet Access from the on-premises network to Microsoft 365. The deployment has the Microsoft 365 profile enabled and contains the following:

- Default traffic policies for Microsoft 365 services
- A linked Conditional Access policy that performs compliant network checks with continuous access evaluation and is applied to all users
- An assignment to all the devices
- An assignment to a remote network associated with the on-premises network

Which Microsoft 365 resources are protected by using continuous access evaluation?

A. SharePoint Online only
B. Exchange Online only
C. both SharePoint Online and Exchange Online

Answer: A

Question: 216

HOTSPOT
You have a Microsoft 365 £5 subscription.
You plan to implement Microsoft Priva Subject Rights Requests for Microsoft 365 data.
You need to streamline the creation and processing of subject rights requests. The solution must minimize development 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

To streamline creation: (The Microsoft Graph API

The Microsoft Graph API

The Microsoft Office 365 Management API

The Microsoft Office 365 service

The Microsoft Office 365 Communications API

To streamline processing I Microsoft Power Automate ,

Azure Automation

Azure Logic Apps

Microsoft Power Automate

Answer:

Explanation:

Answer Area

To streamline creation: [The Microsoft Graph API

To streamline processing: Microsoft Power Automate

Question: 218

HOTSPOT
You have an Azure subscription.
You need to use a federated model in Azure API Management to control access to your organization's APIs. The solution must meet the following requirements:

- Support the use of role-based access control (RBAC) to manage the APIs.
- Support the use of keys to control the consumption of the APIs.

To which scope should you associate each control method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

RBAC roles: ces

Workspa

Products

Subscnptions

Workspaces

Keys: Subscriptions

Products

Subscriptions

Workspaces

Answer:

Explanation:

Answer Area

R8AC roles Workspaces

Keys: Subscriptions

Question: 220

You have a Microsoft Entra tenant named contoso.com.

You have a partner company that has a multi-tenant application named App1. App1 is registered to a Microsoft Entra tenant named fabnkam.com.

You need to ensure that the users in contoso.com can authenticate to App1.

What should you recommend creating in contoso.com?

A. a service principal

B. a system-assigned managed identity

C. an application object

D. a user-assigned managed identity

Answer: A

Explanation:

Question: 221

Your company has on-premises datacenters in Seattle, Chicago, and New York City.

You plan to migrate the on-premises workloads to the East US Azure region.

You need to design a governance solution for the management group hierarchy. The solution must be based on Microsoft Cloud Adoption Framework for Azure principles and must ensure that the hierarchy aligns with the Azure landing conceptual architecture.

What should you use to identify which archetype-aligned management groups to create beneath the landing zones management group?

A. software development lifecycle (SDLQ environments
B. the internal billing chargeback structure
C. the hybrid connectivity requirements
D. geographical locations

Answer: A

Explanation:

Question: 222

Your network contains an Active Directory Domain Services (AD DS) domain.

You need to ensure that the built-in administrator account for the domain can be used only for interactive sign-ins to domain controllers.

What should you configure?

A. the Protected Users group
B. authentication policies
C. the User Rights Assignment security policy settings
D. an authentication policy silo

Answer: B

Explanation:

Question: 223

HOTSPOT

Your on-premises network contains an Active Directory Domain Services (AD DS) domain. The domain contains a group named Group1 and five servers that run Windows Server. Each server contains a standalone app. Each app is used by the members of Group1.

You have a Microsoft Entra tenant that syncs with the domain.

You plan to manage access to the apps by deploying Global Secure Access. You will use a Conditional Access policy to enforce security controls for all connections to the apps.

You need to recommend a Global Secure Access app and Microsoft Entra private network connector configuration for the planned deployment. The solution must minimize administrative effort and be highly available.

What is the minimum number of Global Secure Access apps and private network connectors you should recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Global Secure Access apps Five enterprise applications One enterprise application One Quick Access app

Five enterpnse applications

Five Quick Access apps

1
2
5
10

Private network connectors: 5

Answer:

Explanation:

Answer Area

Global Secure Access apps Five enterprise applications

Private network connectors 5

Question: 224

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 stores documents that are based on a predefined form and include confidential employee information.

You monitor access to Site1 by using a Microsoft Defender for Cloud Apps session policy.

You need to ensure that step-up authentication is triggered when a user downloads documents that are based on the predefined form. The solution must minimize administrative effort.

Which Microsoft Data Classification Service inspection method should you use, and which Conditional Access option should you add to the session policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Inspection method Exact data match (EDM)

Exact data match (EDM)

Fingerprint

Trainable classifier

Option Authentication context I

Authentication context Authentication strength

Custom control

Answer:

Explanation:

Answer Area

Inspection method Exact data match (EDK^

Option: Authentication context

Question: 225

HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a 10- node virtual machine scale set that hosts a web search app named App1. Customers access App1 from the internet. The nodes establish outbound HTTP and HTTPS connections to the internet.

You need to recommend a network security solution for App1. The solution must meet the following requirements:

- Inbound connections to App1 that contain security threats specified in the Core Rule. Set (CRS) from the Open Web Application Security Project (OWASP) must be blocked.
- Outbound HTTP and HTTPS connections from the virtual machine scale set that contain security threats identified by the Microsoft Defender Threat Intelligence (Defender TI) feed must be blocked. What should you include in the recommendation? To answer, select the options in the answer area, NOTE: Each correct answer is worth one point.

Answer Area

For the inbound connections. Azure Web Application Firewall (WAF) ,

Application security groups Azure Firewall

Azure Web Application Firewall (WAF)

Microsoft Entra application proxy Network security groups (NSGs)

For the outbound connections: Azure Firewall _____ | Application security groups

Azure Firewall

Azure Web Application Firewall (WAF)

Microsoft Entra application proxy

Network security groups (NSGs)

Answer:

Explanation:

Answer Area

For the inbound connections. Azure Web Application Firewall (WA

For the outbound connections; Azure Firewall

Question: 226

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. The subscription contains 500 devices that are enrolled in Microsoft Intune. The subscription contains 500 users that connect to external software as a service (SaaS) apps by using the devices.

You need to implement a solution that meets the following requirements:

- Allows user access to SaaS apps that Microsoft has identified as low risk.
- Blocks user access to Saas apps that Microsoft has identified as high risk.

Solution: You configure app protection policies in Intune, and you create a Conditional Access policy. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 227

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. The subscription contains 500 devices that are enrolled in Microsoft Intune. The subscription contains 500 users that connect to external software as a service (SaaS) apps by using the devices.

You need to implement a solution that meets the following requirements:

- Allows user access to SaaS apps that Microsoft has identified as low risk.
- Blocks user access to Saas apps that Microsoft has identified as high risk.

Solution: From Microsoft Defender for Cloud Apps, you configure SaaS security posture management (SSPM)

and create an access policy.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 228

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. The subscription contains 500 devices that are enrolled in Microsoft Intune. The subscription contains 500 users that connect to external software as a service (SaaS) apps by using the devices.

You need to implement a solution that meets the following requirements:

- Allows user access to SaaS apps that Microsoft has identified as low risk.
- Blocks user access to Saas apps that Microsoft has identified as high risk.

Solution: From Microsoft Defender for Cloud Apps, you configure a cloud discovery policy and unsanction risky apps.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 229

You have an Azure subscription and a Microsoft 365 subscription. All users are assigned Microsoft 365 E5 licenses. All computers run Windows 11 and are Microsoft Entra joined.

You need to recommend a solution to prevent computers that run early builds of Windows 11 from connecting to Microsoft 365 services.

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

A. Microsoft Defender for Cloud regulatory compliance policy

B. Microsoft Defender for Endpoint endpoint security policy

C. Microsoft Entra ID Protection sign-in risk policy

D. Microsoft Entra Conditional Access policy

E. Microsoft Intune compliance policy

Answer: D, E

Explanation:

Question: 230

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.

You use Microsoft Defender XDR to manage the tenants of your company's customers.

You need to ensure that the users in Group1 can perform security tasks in the tenant of each customer. The solution must meet the following requirements:

The Group1 users must only be assigned the Security Operator role for the customer tenants.

The users in Group2 must be able to assign the Security Operators role to the Group1 users for the customer tenants.

The use of guest accounts must be minimized.

Administrative effort must be minimized.

What should you include in the solution?

A. Privileged Identity Management (PIM)

B. multi-user authorization (MUA)

C. Microsoft Entra B2B collaboration

D. Azure Lighthouse

Answer: D

Explanation:

Question: 231

HOTSPOT

You have an Azure subscription that contains an Azure key vault named Vault1.

You plan to deploy multiple virtual machines that will host a custom app named App1. App1 will use secrets stored in Vault1. The virtual machines will be redeployed regularly based on the usage demands of App1.

You need to recommend a solution that will enable App1 to access the secrets stored in Vault1. The solution must meet the following requirements:

Minimize the number of security principals that can access Vault1.

Minimize the storage of sensitive data on the virtual machines.

Minimize administrative effort.

Which type of endpoint should App1 use to access the secrets, and which type of identity should App1 use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Fndpoint type *

Azure Instance Metadata Service (1MDS)

Identity type: M*,^ G<aph REST AM el B

Microsoft Identity Platform OAulh 10 access token

Identity type *

Service principal

System-assigned managed identity

User assigned managed Identity

Answer:

Explanation:

www.atmicnetworks.com

Question: 232

HOTSPOT

You have four Azure subscriptions named Sub1, Sub2, Sub3, and Sub4. Each subscription has a unique Microsoft Entra tenant that is linked to a Microsoft 365 subscription. Sub1 contains a user named User1.

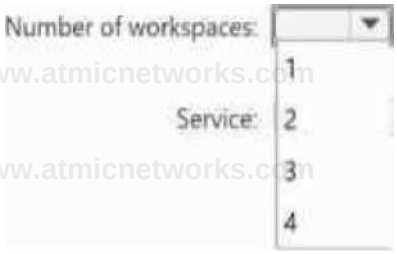
You plan to implement Microsoft Sentinel.

You need to ensure that User1 can monitor Microsoft Entra ID events and Microsoft 365 events for Sub2, Sub3, and Sub4 by using Microsoft Sentinel. The solution must minimize administrative effort.

What is the minimum number of Microsoft Sentinel workspaces you should create, and which Azure service should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Service

Answer:

Explanation:

Answer Area

Question: 233

Your on-premises network contains an Active Directory Domain Services (AD DS) domain. The domain contains 500 Windows 11 devices.

You have a Microsoft 365 subscription and an Azure subscription.

You have a Microsoft Entra tenant that syncs with the domain and is linked to the subscriptions. The devices are Microsoft Entra hybrid joined.

You plan to deploy a solution to mitigate attacks against privileged accounts. The solution will include Microsoft Sentinel rules that will detect attempts to use fake cached credentials.

You need to recommend a solution to create the fake cached credentials on client computers.

What should you recommend?

A. User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

B. a deception rule in Microsoft Defender for Endpoint

C. a Honeytoken tag in Microsoft Defender for Identity

D. a user risk policy in Microsoft Entra ID Protection

Answer: B

Explanation:

Question: 234

HOTSPOT

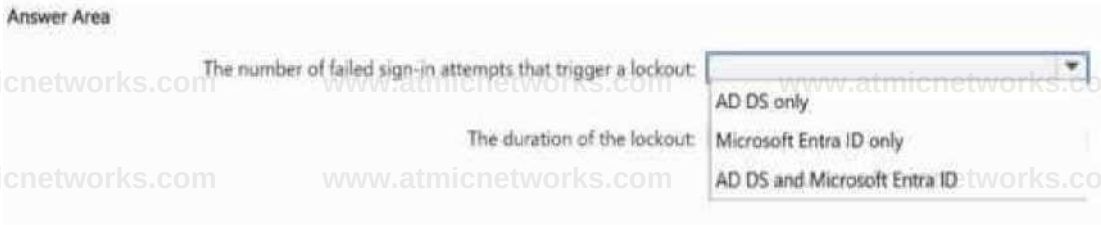
Your network contains an Active Directory Domain Services (AD DS) domain named Domain1.

You have a Microsoft Entra tenant.

Domain1 syncs with the tenant by using Microsoft Entra Connect.

You need to evaluate Microsoft Entra smart lockout by testing the following account lockout considerations:

The number of failed sign-in attempts that trigger a lockout.



Answer:

Explanation:

Answer Area

The number al laded sign-in attempts that trigger a lockout AD DS and Microsoft Entra ID

The duration of the lockout AD DS and Microsoft Entra ID

Question: 235

You have a Microsoft Entra tenant named contoso.com.

You have an external partner that has a Microsoft Entra tenant named fabrikam.com.

You need to recommend an identity governance solution for contoso.com that meets the following requirements:

Enables the users in contoso.com and fabrikam.com to communicate by using shared Microsoft Teams channels.

Manages access to shared Teams channels in contoso.com by using groups in fabrikam.com.

Supports single sign-on (SSO).

Minimizes administrative effort.

Maximizes security.

What should you include in the recommendation?

A. Microsoft Entra B2B collaboration

B. Microsoft Entra Connect Sync

C. Cross-tenant synchronization

D. B2B direct connect

Answer: D

Explanation:

Question: 236

HOTSPOT

You have an Azure subscription. The subscription contains 20 App Service web apps that provide services to external customers.

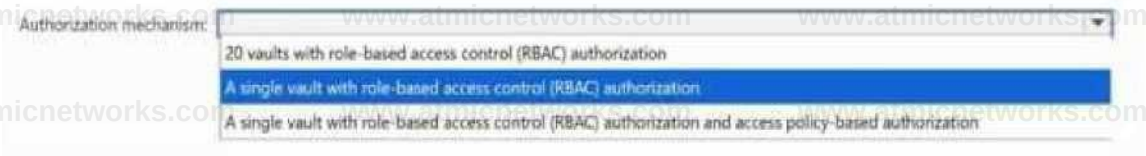
Each web app has a unique certificate and key.

You need to recommend a solution to manage the keys and certificates of the web apps. The solution must meet the follow requirements:

Provide a single tenancy to store the keys and certificates.

Maintain FIPS 140-2 Level 3 compliance.

Follow the principle of least privilege.



Answer:

Explanation:

Answer Area

Azure service Azure Key Vault Managed HSM

Authorization mechanism A single vault with role-based access control (R8AC) authorization

Question: 237

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)

Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the onpremises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Application Gateway v2 with user-defined routes (UDRs)

C. Azure Front Door with Azure Web Application Firewall (WAF)

D. Azure Firewall with policy rule sets

Answer: D

Explanation:

Question: 238

You have a Microsoft 365 subscription that contains a group named Group1. The subscription contains 1,000 Windows devices that are joined to a Microsoft Entra tenant and managed by using Microsoft Intune. All users sign in to the devices by using standard user accounts.

You plan to deploy a new app named App1 to the members of Group1. The Group1 members must have administrative rights to install new versions of App1.

You need to ensure that the Group1 members can install new versions of App1. The solution must follow the principles of Zero Trust.

What should you implement?

A. Microsoft Local Administrator Password Solution (Microsoft LAPS)

B. Endpoint Privilege Management (EPM)

C. Privileged Identity Management (PIM)

D. Microsoft Entra entitlement management

Answer: B

Explanation:

Question: 239

You have an Azure subscription that contains multiple Azure Blob Storage accounts.

You need to recommend a solution to detect threats in files after the files are uploaded to a blob container.

What should you include in the recommendation?

A. vulnerability assessment in Microsoft Defender for Containers

B. runtime threat protection in Microsoft Defender for Containers

C. malware scanning in Microsoft Defender for Storage

D. sensitive data threat detection in Microsoft Defender for Storage

Answer: C

Explanation:

www.atmicnetworks.com

Question: 241

HOTSPOT

You have an Azure subscription that contains an Azure Synapse Analytics workspace named workspace1. workspace1 contains a built-in serverless SQL pool and a dedicated SQL pool named Pool1.

You need to recommend a second layer of data encryption for workspace1.

What should you include in the recommendation for each pool? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Pool!

Infrastructure encryption

Serverfess SQL pool Server side encryption (SSE)

Transparent Data Encryption (TDE)

Serverless SQL pool

Infrastructure encryption

Server-side encryption (SSE)

Transparent Data Encryption (TDE)

Answer:

Explanation:

Answer Area

Pool! Infrastructure encryption

Serverless SQL pool Server side encryption (SSE)

www.atmicnetworks.com

Question: 242

DRAG DROP

For a Microsoft cloud environment, you need to recommend a security architecture that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security methodologies should you include in the recommendation? To answer, drag the appropriate methodologies to the

correct principles. Each methodology 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.

Answer:

Explanation:

Question: 243

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. Active Directory Domain Services (AD DS)

B. Microsoft Entra ID

C. Microsoft Entra Domain Services

D. Microsoft Entra External ID

Answer: B

Explanation:

Question: 244

You have an Azure subscription and a Microsoft 365 subscription.

Your company uses several software as a service (SaaS) applications.

To align with Microsoft cloud security benchmark (MCSB) and Microsoft Cybersecurity Reference Architectures (MCRA), you plan to design a solution to provide visibility into user activity across the applications and detect potentially risky behavior in real time.

Which service should you recommend?

A. Microsoft Purview Information Protection

B. Microsoft Defender for Cloud Apps

C. Microsoft Defender for Endpoint

D. Microsoft Sentinel

Answer: B

Explanation:

Question: 245

HOTSPOT

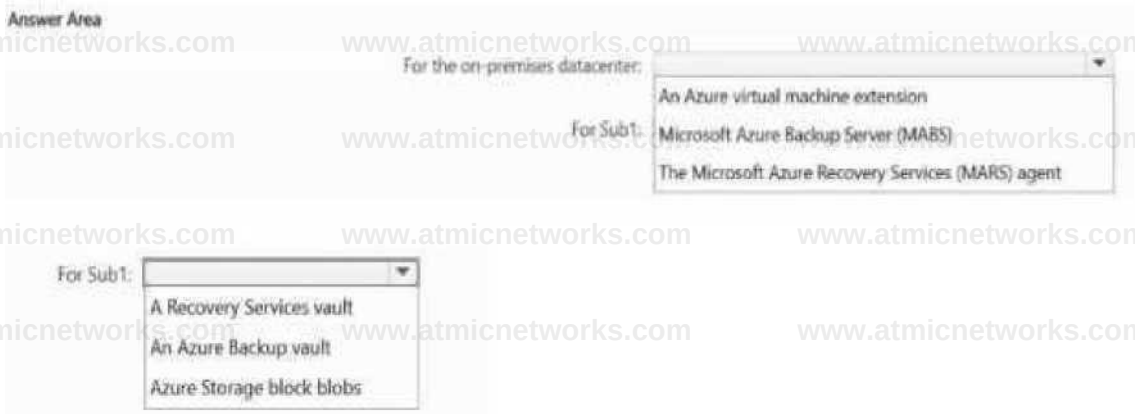
You have an on-premises datacenter. The datacenter contains a server named Server1 that runs Windows Server 2022 and a firewall that prevents Server1 from connecting to the internet.

You have an Azure subscription named Sub1.

You need to recommend a resiliency strategy for Server1 that incorporates a backup plan to transfer the data from Server1 to Sub1.

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:

Explanation:

Question: 246

You have an Azure subscription.

You have a subscription to a third-party cloud provider. The subscription contains 100 virtual machines.

You manage cloud security for both subscriptions from the Azure subscription.

You need to recommend a solution to validate the security posture of the virtual machines.

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

A. Microsoft Defender for Cloud

B. Microsoft Defender for Endpoint

C. Azure Lighthouse

D. Microsoft Sentinel

E. Azure Arc

Answer: A, E

www.atmicnetworks.com