SC-100 Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

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, databases, files, and storage accounts.

What should you include in the recommendation?

A. business resilience

B. modem access control

C. network isolation

D. security baselines in the Microsoft Cloud Security Benchmark

Correct Answer: D

Explanation:

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multi-cloud environment. This benchmark focuses

on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

Controls include:

*

Endpoint Security (ES)

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in cloud environments.

*

Data Protection (DP)

Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key management and

certificate management.

*

Etc.

Reference: https://learn.microsoft.com/en-us/security/benchmark/azure/overview

QUESTION 2

HOTSPOT

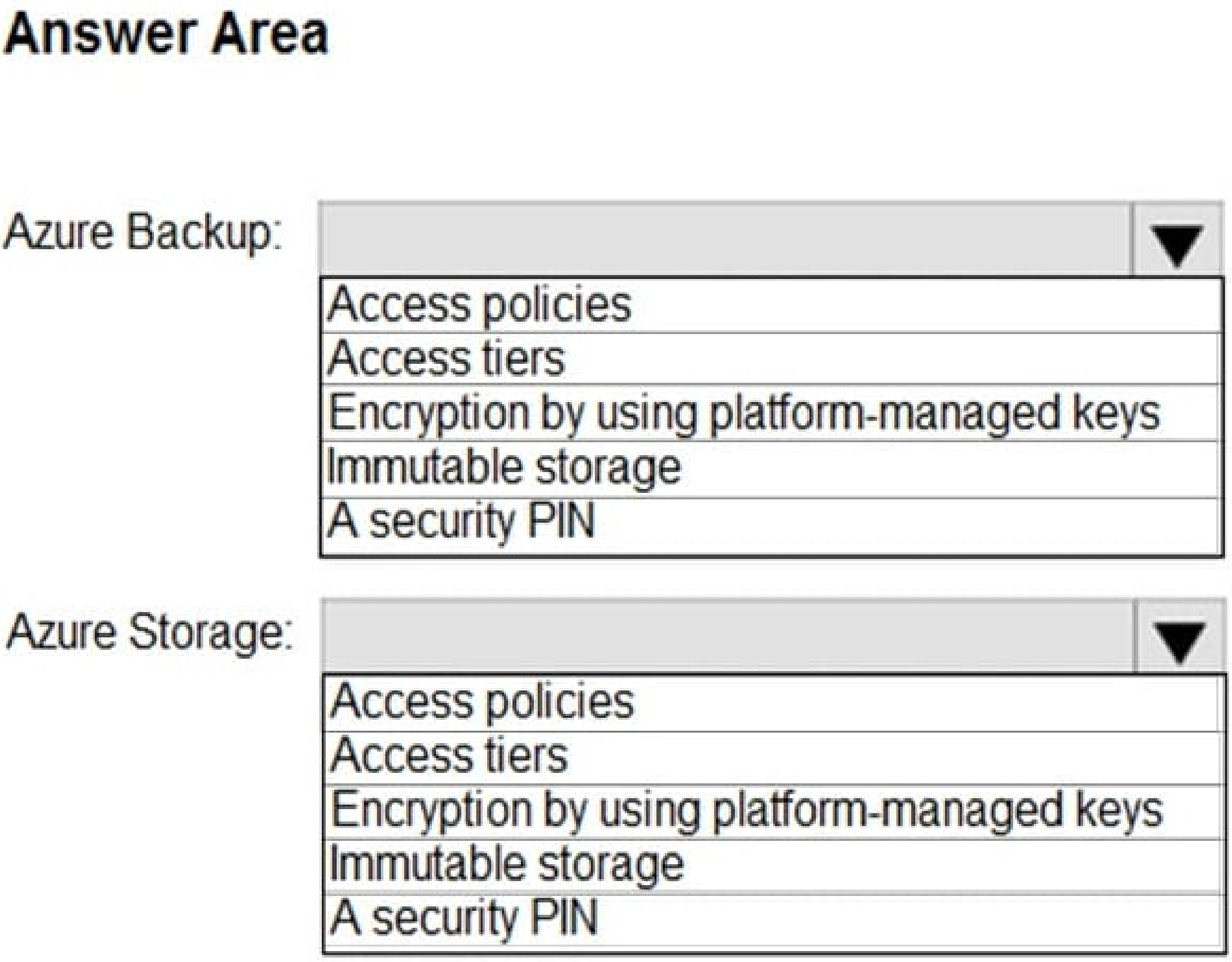
Your company wants to optimize using Azure to protect its resources from ransomware.

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.

Hot Area:

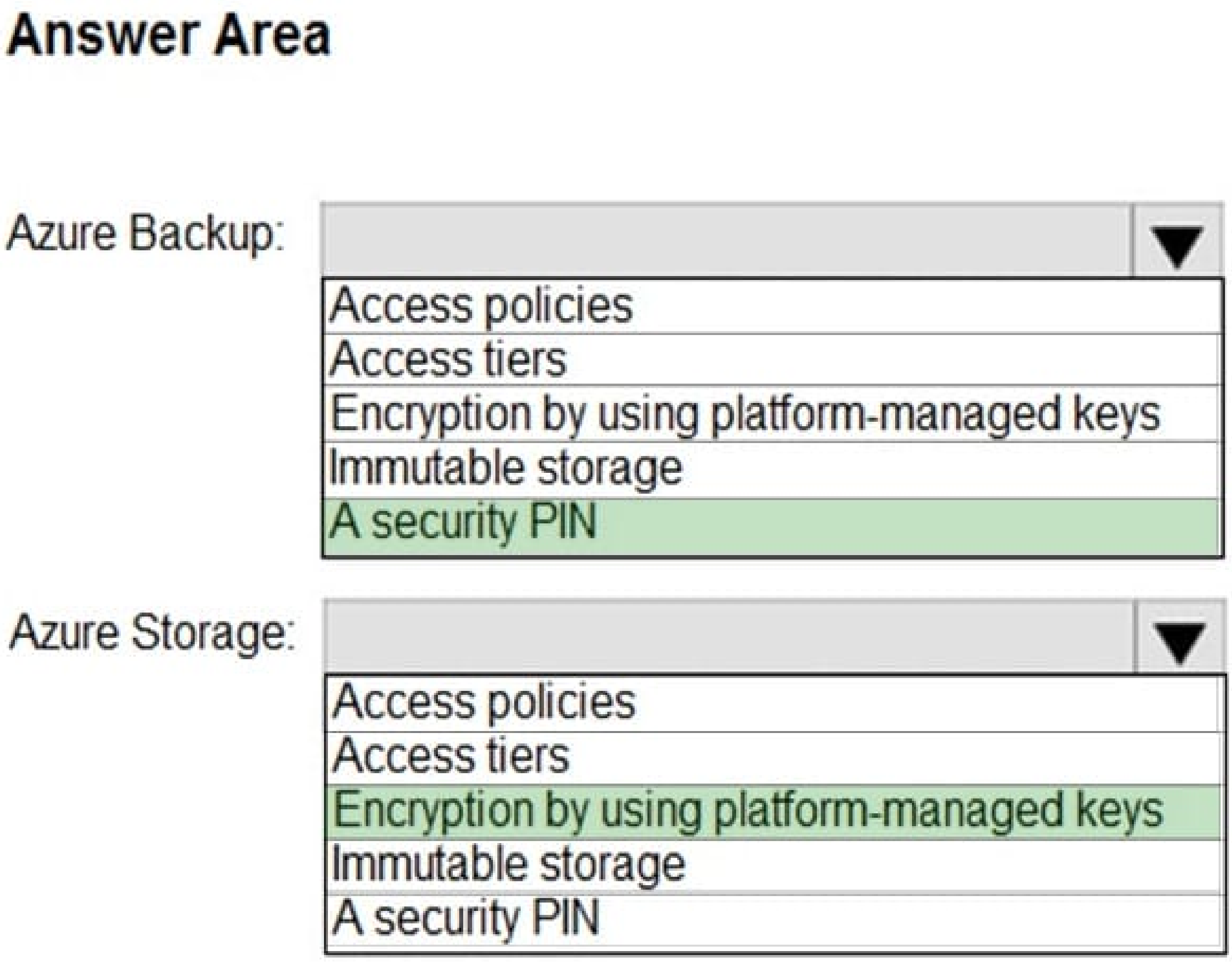


Answer Area

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

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

Correct Answer:



Answer Area

Azure Backup:

- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- [✓ A security PIN]

Azure Storage:

- Access policies
- Access tiers
- [✓ Encryption by using platform-managed keys]
- Immutable storage
- A security PIN

Box 1: A security PIN

Azure Backup

The best way to prevent falling victim to ransomware is to implement preventive measures and have tools that protect your organization from every step that attackers take to infiltrate your systems.

You can reduce your on-premises exposure by moving your organization to a cloud service.

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a

security PIN before modifying online backups.

Box 2: Encryption by using platform-managed keys

Ensure backup data is encrypted.

By default, backup data at rest is encrypted using platform-managed keys (PMK). For vaulted backups, you can choose to use customer-managed keys (CMK) to own and manage the encryption keys yourself. Additionally, you can configure

encryption on the storage infrastructure using infrastructure-level encryption, which along with CMK encryption provides double encryption of data at rest.

Reference:

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

https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

QUESTION 3

HOTSPOT

You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:

1.

Users will authenticate by using Azure AD user accounts.

2.

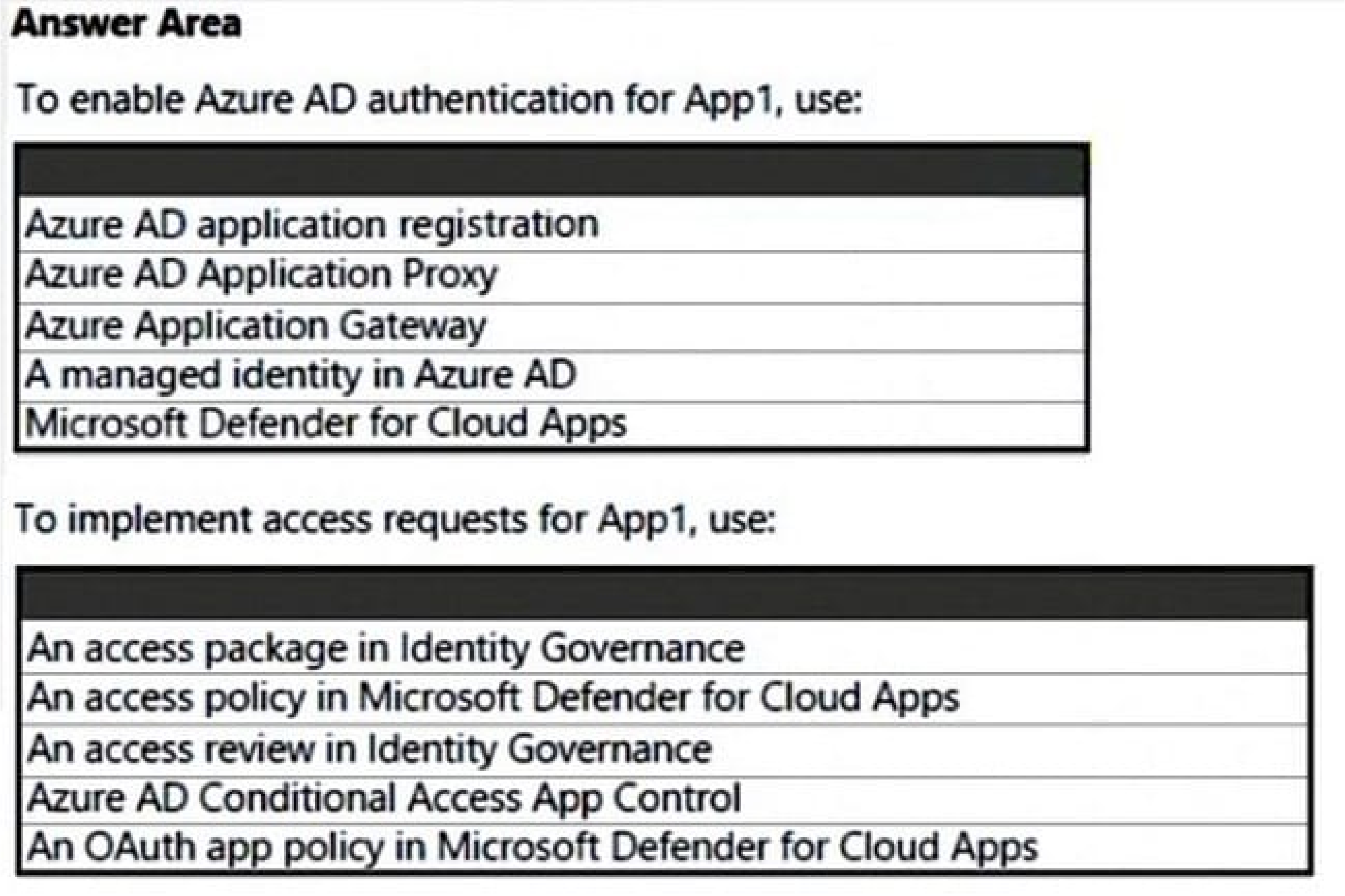
Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.

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.

Hot Area:



Answer Area

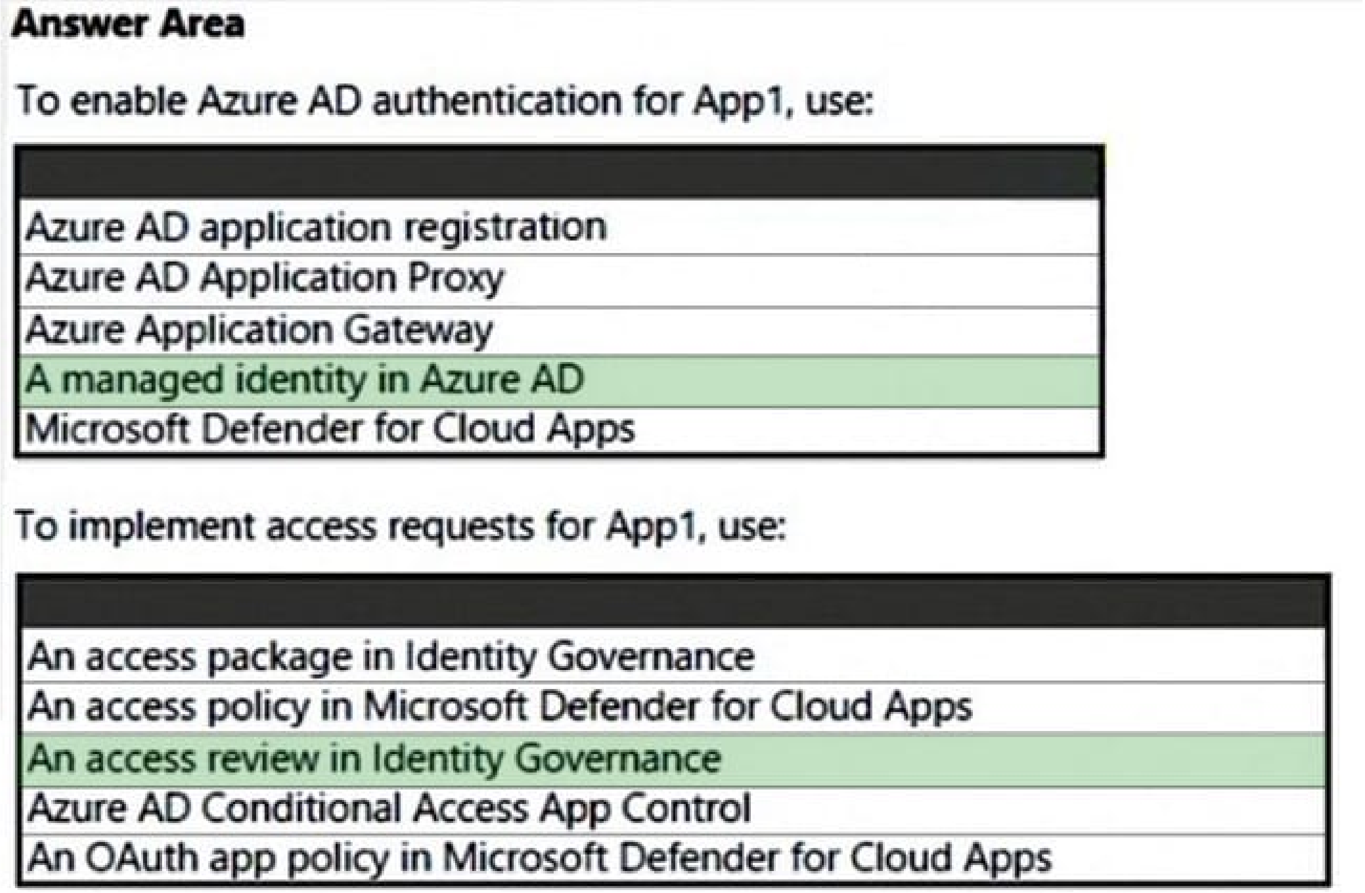
To enable Azure AD authentication for App1, use:

- Azure AD application registration
- Azure AD Application Proxy
- Azure Application Gateway
- A managed identity in Azure AD
- Microsoft Defender for Cloud Apps

To implement access requests for App1, use:

- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- An access review in Identity Governance
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

Correct Answer:



Answer Area

To enable Azure AD authentication for App1, use:

- Azure AD application registration
- Azure AD Application Proxy
- Azure Application Gateway
- [✓ A managed identity in Azure AD]
- Microsoft Defender for Cloud Apps

To implement access requests for App1, use:

- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- [✓ An access review in Identity Governance]
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

Box 1: A managed identity in Azure AD

Use a managed identity. You use Azure AD as the identity provider.

Box 2: An access review in Identity Governance

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group

members or application access.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

QUESTION 4

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 Firewall, 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 Well-Architected Framework

C. Azure Security Benchmark v3

D. Azure Advisor

Correct Answer: A

Explanation:

About Azure Bastion host and jumpboxes

The most simple solution is to host a jumpbox on the virtual network of the data management landing zone or data landing zone to connect to the data services through private endpoints.

Azure Bastion provides a few other core security benefits, including:

*

The service integrates with native security appliances for an Azure virtual network, such as Azure Firewall.

Note:

*

Platform landing zones: Subscriptions deployed to provide centralized services, often operated by a central team, or a number of central teams split by function (e.g. networking, identity), which will be used by various workloads and applications. Platform landing zones represent key services that often benefit from being consolidated for efficiency and ease of operations. Examples include networking, identity, and management services.

*

The Azure App Service landing zone accelerator is an open-source collection of architectural guidance and reference implementation to accelerate deployment of Azure App Service at scale. It can provide a specific architectural approach and reference implementation via infrastructure as code templates to prepare your landing zones. The landing zones adhere to the architecture and best practices of the Cloud Adoption Framework.

Incorrect:

Not B: The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architectural excellence:

Reliability Security Cost Optimization Operational Excellence Performance Efficiency

Not C: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance that also includes:

*

Cloud Adoption Framework: Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.

*

Azure Well-Architected Framework: Guidance on securing your workloads on Azure.

*

Microsoft Security Best Practices: Recommendations with examples on Azure.

Microsoft Cybersecurity Reference Architectures (MCRA): Visual diagrams and guidance for security components and relationships

*

The Azure Security Benchmark focuses on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls, National Institute of

Standards and Technology (NIST), and Payment Card Industry Data Security Standard (PCI-DSS).

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/cloud-scale-analytics/architectures/connect-to-environments-privately

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v3

https://learn.microsoft.com/en-us/azure/architecture/framework/

QUESTION 5

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. Enable soft delete for backups.

B. Require PINs for critical operations.

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

D. Perform offline backups to Azure Data Box.

E. Use Azure Monitor notifications when backup configurations change.

Correct Answer: BE

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a security PIN before modifying online backups.

Your backups need to be protected from sophisticated bot and malware attacks. Permanent loss of data can have significant cost and time implications to your business. To help protect against this, Azure Backup guards against malicious attacks through deeper security, faster notifications, and extended recoverability.

For deeper security, only users with valid Azure credentials will receive a security PIN generated by the Azure portal to allow them to backup data. If a critical backup operation is authorized, such as “delete backup data,” a notification is immediately sent so you can engage and minimize the impact to your business. If a hacker does delete backup data, Azure Backup will store the deleted backup data for up to 14 days after deletion.

E: Key benefits of Azure Monitor alerts include:

Monitor alerts at-scale via Backup center: In addition to enabling you to manage the alerts from Azure Monitor dashboard, Azure Backup also provides an alert management experience tailored to backups via Backup center. This allows you

to filter alerts by backup specific properties, such as workload type, vault location, and so on, and a way to get quick visibility into the active backup security alerts that need attention.

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
https://www.microsoft.com/security/blog/2017/01/05/azure-backup-protects-against-ransomware/
https://docs.microsoft.com/en-us/azure/backup/move-to-azure-monitor-alerts

QUESTION 6

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

All 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 solutions to meet the following requirements:

1.

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

2.

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

A. a custom collector that uses the Log Analytics agent

B. the Azure Monitor agent

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

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

Correct Answer: BC

A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data

during collection to individual fields.

You can connect your data sources to Microsoft Sentinel using custom log formats.

C: Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel. The different roles give you fine-grained control over what Microsoft Sentinel users can see and do. Azure

roles can be assigned in the Microsoft Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel inherits.

Incorrect:

A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.

You can connect your data sources to Microsoft Sentinel using custom log formats.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview https://docs.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG https://docs.microsoft.com/en-us/azure/sentinel/roles

QUESTION 7

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. active scanning

B. threat monitoring

C. software patching

D. passive traffic monitoring

Correct Answer: BC

Explanation: Microsoft Cybersecurity Reference Architectures Apply zero trust principles to securing OT and industrial IoT environments

Operational Technology (OT) Environments Safety/Integrity/Availability

- Hardware Age: 50-100 years (mechanical + electronic overlay)
- Warranty length: up to 30-50 years
- Protocols: Industry Specific (often bridged to IP networks)
- Security Hygiene: Isolation, threat monitoring, managing vendor access risk, (patching rarely)

Information Technology (IT) Environments Confidentiality/Integrity/Availability

- Hardware Age: 5-10 years
- Warranty length 3-5 years
- Protocols: Native IP, HTTP(S), Others
- Security Hygiene: Multi-factor authentication (MFA), patching, threat monitoring, antimalware

Reference: https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

QUESTION 8

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

Correct Answer: B

Explanation:

Securing Azure Pipelines

YAML pipelines offer the best security for your Azure Pipelines. In contrast to classic build and release pipelines, YAML pipelines:

*

Can be code reviewed. YAML pipelines are no different from any other piece of code. You can prevent malicious actors from introducing malicious steps in your pipelines by enforcing the use of Pull Requests to merge changes. Branch policies make it easy for you to set this up.

*

Etc.

Reference: https://learn.microsoft.com/en-us/azure/devops/pipelines/security/overview

QUESTION 9

HOTSPOT

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

You need to evaluate the existing environment to increase the overall security posture for the following components:

1.

Windows 11 devices managed by Microsoft Intune

2.

Azure Storage accounts

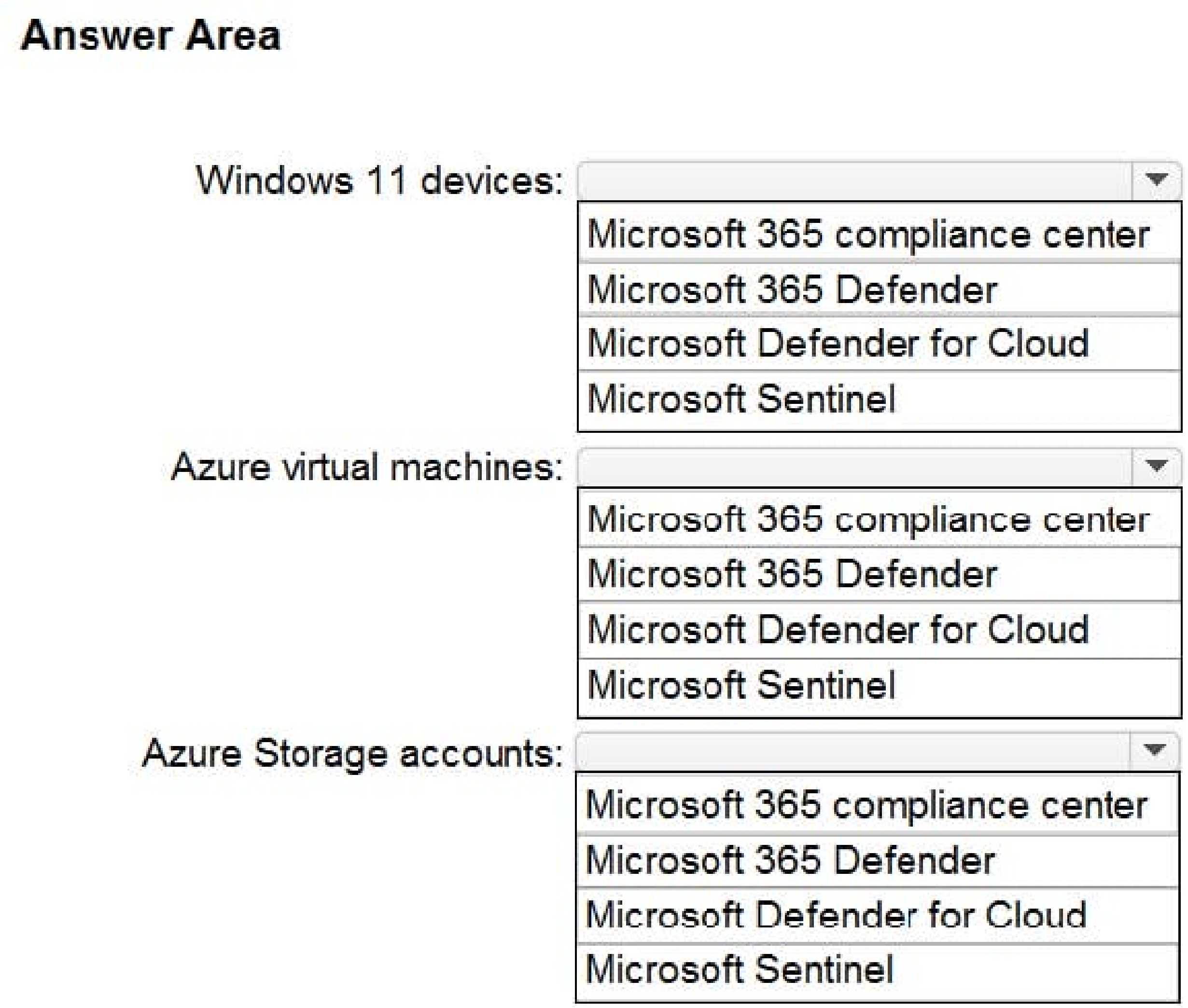
3.

Azure virtual machines

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

NOTE: Each correct selection is worth one point.

Hot Area:



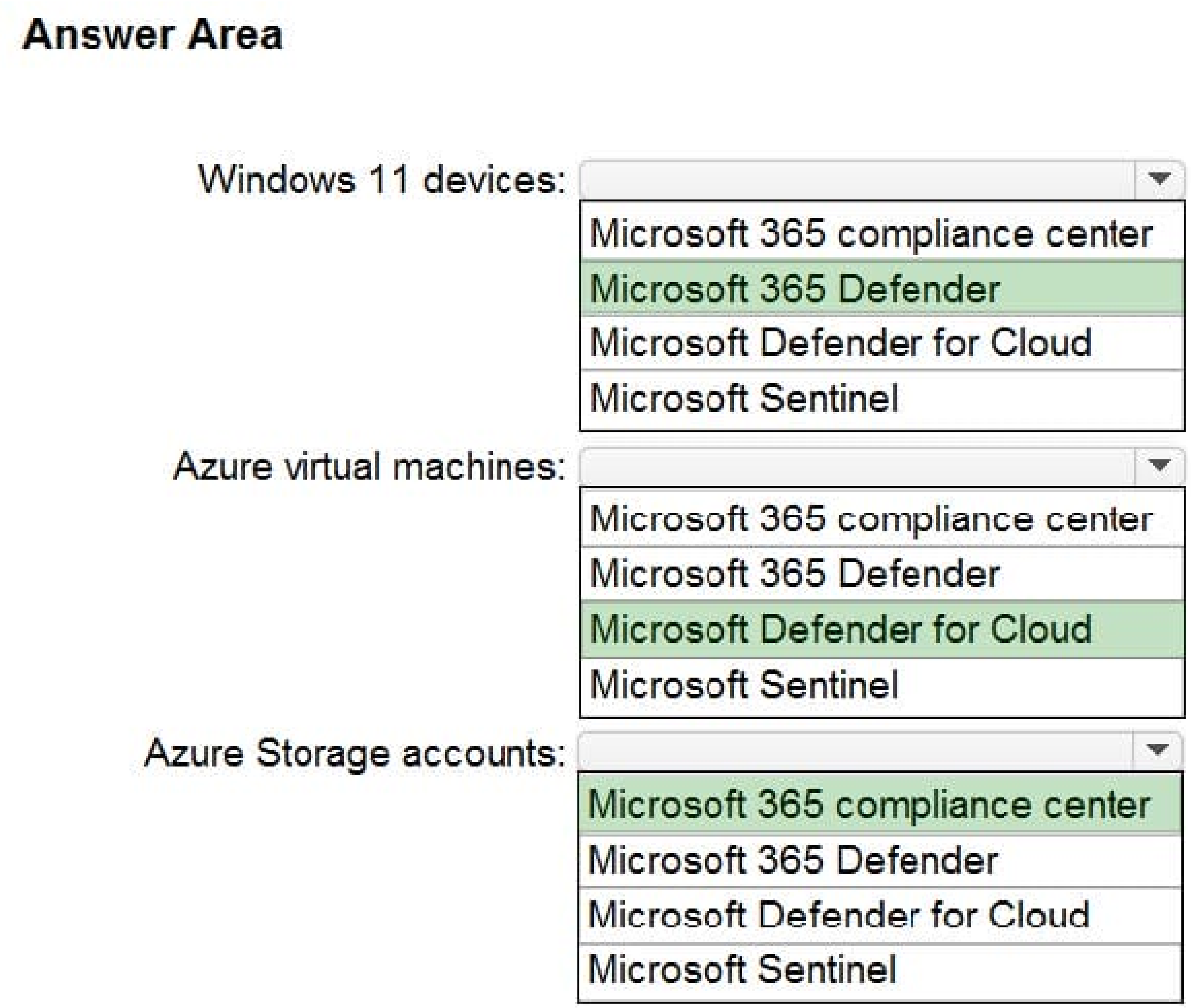
Answer Area

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

Correct Answer:



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

Box 1: Microsoft 365 Defender

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Microsoft Defender for Endpoint works with devices that run:

Android

iOS/iPadOS

Windows 10

Windows 11

Box 2: Microsoft Defender for Cloud

Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed

Instance and Azure Virtual Machines.

Box 3: Microsoft 365 Compliance Center

Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.

Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.

Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.

Reference: https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint

https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

QUESTION 10

HOTSPOT

Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS).

You need to recommend an identity security strategy that meets the following requirements:

1.

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

2.

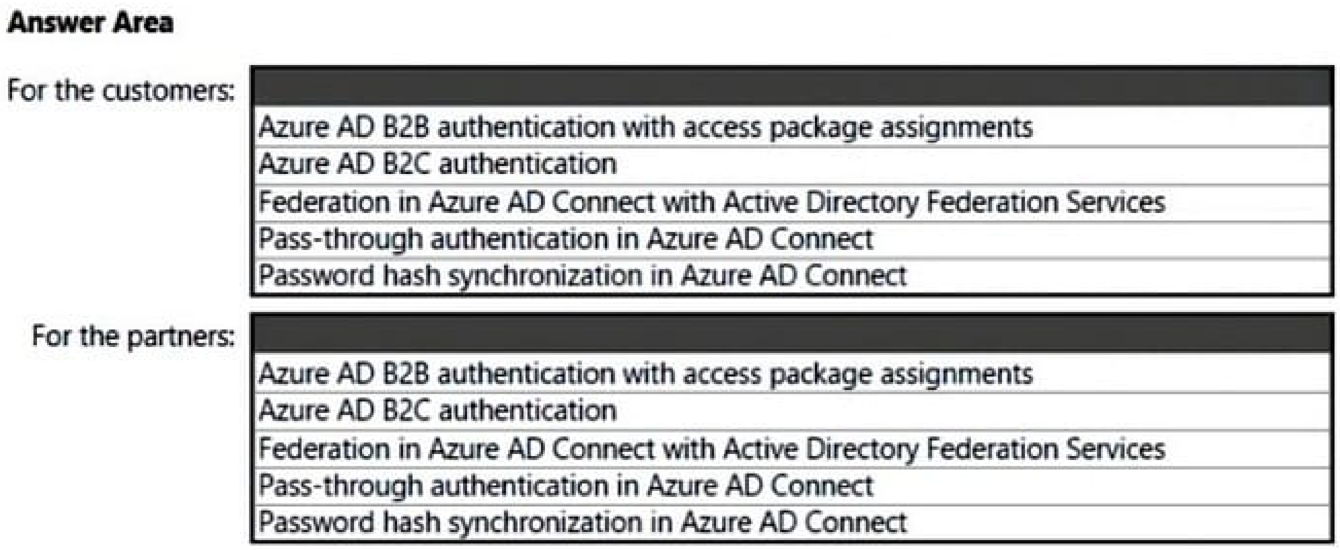
Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

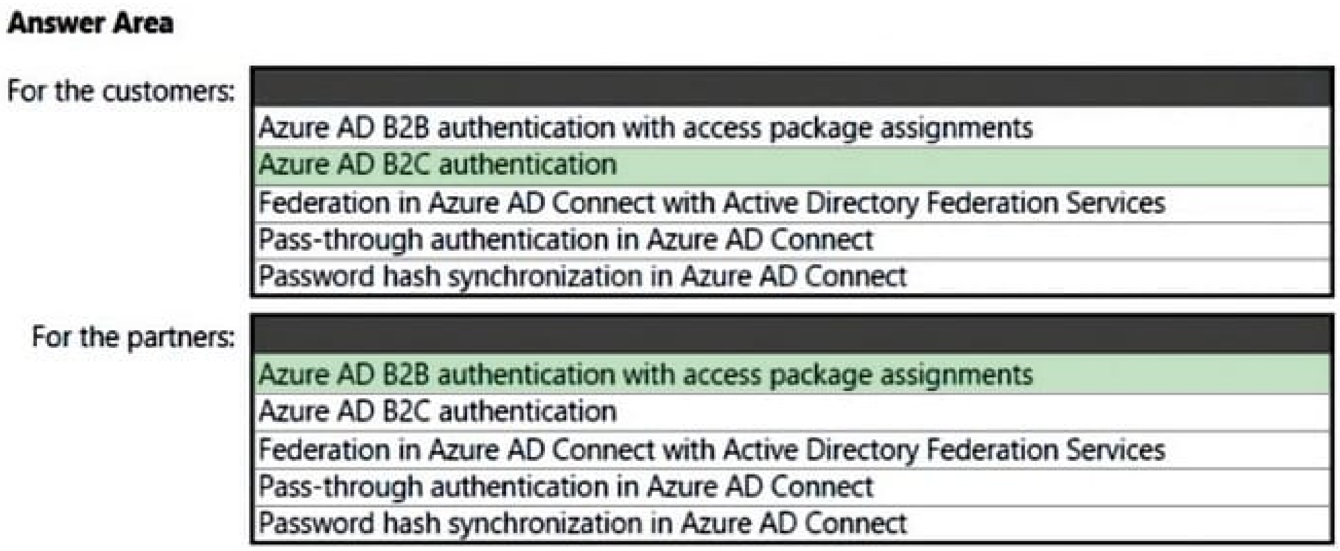
For the customers:

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

For the partners:

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

Correct Answer:



Answer Area

For the customers:

Azure AD B2B authentication with access package assignments
[✓ Azure AD B2C authentication]
Federation in Azure AD Connect with Active Directory Federation Services
Pass-through authentication in Azure AD Connect
Password hash synchronization in Azure AD Connect

For the partners:

[✓ Azure AD B2B authentication with access package assignments]
Azure AD B2C authentication
Federation in Azure AD Connect with Active Directory Federation Services
Pass-through authentication in Azure AD Connect
Password hash synchronization in Azure AD Connect

Box 1: Azure AD B2C authentication

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website.

You can set up sign-up and sign-in with a Facebook account using Azure Active Directory B2C.

Box 2: Azure AD B2B authentication with access package assignments

Govern access for external users in Azure AD entitlement management

Azure AD entitlement management uses Azure AD business-to-business (B2B) to share access so you can collaborate with people outside your organization. With Azure AD B2B, external users authenticate to their home directory, but have a

representation in your directory. The representation in your directory enables the user to be assigned access to your resources.

Incorrect:

Not: Password hash synchronization in Azure AD connect

The partners are not integrated with AD DS.

Reference: 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/governance/entitlement-management-external-users

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration

QUESTION 11

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

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. Disable Microsoft OneDrive sync and Exchange ActiveSync.

Correct Answer: D

The following containment steps can be done concurrently as new threat vectors are discovered.

Step 1: Assess the scope of the situation

Which user accounts were compromised?

Which devices are affected? Which applications are affected? Step 2: Preserve existing systems

*

Disable all privileged user accounts except for a small number of accounts used by your admins to assist in resetting the integrity of your AD DS infrastructure. If a user account is believed to be compromised, disable it immediately.

*

Isolate compromised systems from the network, but do not shut them off.

*

Etc.

Note:

With OneDrive, you can sync files between your computer and the cloud, so you can get to your files from anywhere - your computer, your mobile device, and even through the OneDrive website at OneDrive.com.

ActiveSync is a client protocol that lets users synchronize their Exchange mailbox with a mobile device.

Reference: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

QUESTION 12

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. SQL Server on Azure Virtual Machines

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

Correct Answer: C

Explanation:

Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking. Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

Azure SQL Database is cheaper as its offer DTU\\'s based tier and also vCore based for more intensive workflow.

Hovewer, Managed Instance offers almost ~100% compatibility with on-prem Microsoft SQL Server.

Incorrect:

Not A: SQL Server does not support dynamic data masking.

Not B: Synapse Analytics is more expensive compared to Azure SQL Database.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

https://learn.microsoft.com/en-us/answers/questions/1057631/azure-sql-db-vs-azure-sql-managed-instance-cost

QUESTION 13

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 AKS1. 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 private endpoint

B. a network security group (NSG)

C. a service endpoint

D. an authorized IP range

Correct Answer: D

Explanation:

By default, the Kubernetes API server uses a public IP address and a fully qualified domain name (FQDN). You can limit access to the API server endpoint using authorized IP ranges. You can also create a fully private cluster to limit API

server access to your virtual network.

Reference:

https://learn.microsoft.com/en-us/azure/aks/concepts-security

QUESTION 14

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. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Correct Answer: ACE

RaMP initiatives for Zero Trust

To rapidly adopt Zero Trust in your organization, RaMP offers technical deployment guidance organized in these initiatives.

Critical security modernization initiatives:

(C) User access and productivity

1. Explicitly validate trust for all access requests Identities Endpoints (devices) Apps Network

(A) Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

(E) Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

reduce manual effort

Incorrect:

As needed

Additional initiatives based on Operational Technology (OT) or IoT usage, on-premises and cloud adoption, and security for in-house app development:

*

(not D) OT and Industrial IoT Discover Protect Monitor

*

Datacenter and DevOps Security Security Hygiene Reduce Legacy Risk DevOps Integration Microsegmentation

Reference: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

---

QUESTION 15

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. Microsoft Sentinel threat intelligence workbooks

B. Microsoft Sentinel notebooks

C. threat intelligence reports in Defender for Cloud

D. workload protections in Defender for Cloud

Correct Answer: AC

A: Workbooks provide insights about your threat intelligence

Workbooks provide powerful interactive dashboards that give you insights into all aspects of Microsoft Sentinel, and threat intelligence is no exception. You can use the built-in Threat Intelligence workbook to visualize key information about

your threat intelligence, and you can easily customize the workbook according to your business needs. You can even create new dashboards combining many different data sources so you can visualize your data in unique ways. Since

Microsoft Sentinel workbooks are based on Azure Monitor workbooks, there is already extensive documentation available, and many more templates.

C: What is a threat intelligence report?

Defender for Cloud\\'s threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to

identify threats.

Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:

Activity Group Report: provides deep dives into attackers, their objectives, and tactics.

Campaign Report: focuses on details of specific attack campaigns.

Threat Summary Report: covers all of the items in the previous two reports.

This type of information is useful during the incident response process, where there\\'s an ongoing investigation to understand the source of the attack, the attacker\\'s motivations, and what to do to mitigate this issue in the future.

Incorrect:

Not B: When to use Jupyter notebooks

While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data.

For example, use notebooks to:

Perform analytics that aren\\'t provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features

Create data visualizations that aren\\'t provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees

Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

Not D: Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through Microsoft

Defender plans specific to the types of resources in your subscriptions. For example, you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your Azure Storage accounts.

Reference: 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