

Microsoft.SC-100.v2026-10-17.q137

Exam Code:	SC-100
Exam Name:	Microsoft Cybersecurity Architect
Certification Provider:	Microsoft
Free Question Number:	137
Version:	v2026-10-17
# of views:	113
# of Questions views:	1707
https://www.freecram.net/torrent/Microsoft.SC-100.v2026-10-17.q137.html	

NEW QUESTION: 1

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. an internet access traffic forwarding profile
- B. a private access traffic forwarding profile
- C. a Global Secure Access app
- D. a Quick Access app

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 3

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

You need to recommend a solution to enforce the Zero Trust principle of explicit verification for the subscriptions. The solution must be based on Zero Trust guidance in the Microsoft Cybersecurity Reference Architectures (MCRA).

What should you include in the recommendation?

- A. Microsoft Defender for Cloud
- B. Microsoft Defender for Identity
- C. Conditional Access
- D. Microsoft Entra ID Identity Governance

Answer: (SHOW ANSWER)

NEW QUESTION: 4

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 Intune compliance policy
- B. Microsoft Entra ID Protection sign-in risk policy
- C. Microsoft Entra Conditional Access policy
- D. Microsoft Defender for Endpoint endpoint security policy
- E. Microsoft Defender for Cloud regulatory compliance policy

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 5

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: (SHOW ANSWER)

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

NEW QUESTION: 6

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. 2

B. 1

C. 3

D. 4

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

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:

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

Explanation:



NEW QUESTION: 8

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: ([SHOW ANSWER](#))

NEW QUESTION: 9

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. a user risk policy in Microsoft Entra ID Protection
- B. a deception rule in Microsoft Defender for Endpoint
- C. a Honeytokens tag in Microsoft Defender for Identity
- D. User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 10

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

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 Sentinel
- C.** Azure Lighthouse
- D.** Azure Arc
- E.** Microsoft Defender for Endpoint

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

You have an Azure subscription.

You plan to deploy an Azure App Service web app named App1 that will access an external web service by using a username and password.

You need to recommend a password storage solution for App1 that meets the following requirements:

* Ensures that the password is stored securely

* Ensures that App1 can authenticate to the service that will store the password Which service should you use to store the password, and which authentication method should App1 use to access the service? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Service:
Microsoft Entra ID Protection
Privileged Identity Management (PIM)

Authentication method:
Group managed service account (gMSA)
Guest account
Managed identity

Answer:

Answer Area

Service:
Microsoft Entra ID Protection
Privileged Identity Management (PIM)

Authentication method:
Group managed service account (gMSA)
Guest account
Managed identity

Explanation:

Answer Area

Service:

Authentication method:

You have an Azure subscription.

You have a Microsoft 365 subscription.

You need to assess regulatory compliance of the subscriptions. The solution must meet the following requirements:

- * Identify whether data stored in Azure and Microsoft 365 complies with General Data Protection Regulation (GDPR) regulations.
- * Identify whether Azure resources comply with National Institute of Standards and Technology (NIST) standards.
- * Provide recommendations on controls to improve compliance.

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

NOTE: Each correct selection is worth one point.

Answer Area

For NIST:

- Microsoft Defender for Cloud
- Microsoft Defender Vulnerability Management
- Microsoft Sentinel

For GDPR:

- Microsoft Priva
- Microsoft Purview Communication Compliance
- Microsoft Purview Compliance manager

Answer:

For NIST: Microsoft Sentinel

For GDPR: Microsoft Purview Compliance manager

Explanation:

Answer Area

For NIST: Microsoft Sentinel

For GDPR: Microsoft Purview Compliance Manager

NEW QUESTION: 15

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 16

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: ([SHOW ANSWER](#)**)**

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview>

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (**343** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

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: ([SHOW ANSWER](#)**)**

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

NEW QUESTION: 18

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. modern security operations
- D. infrastructure and development
- E. operational technology (OT) and IoT

Answer: (SHOW ANSWER)

NEW QUESTION: 19

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: (SHOW ANSWER)

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-worldwide

NEW QUESTION: 20

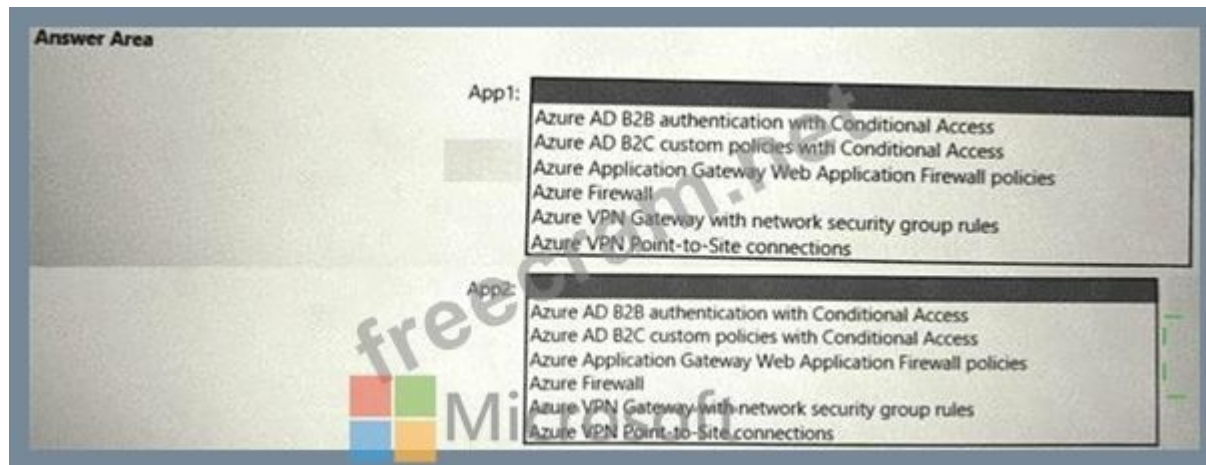
You have a hybrid cloud infrastructure. You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 21

You have an Azure subscription that contains the Azure Virtual Machine Scale Sets shown in the following table.

Name	Configuration
VMSS1	- Orchestration mode: Flexible - Image type: Windows Server virtual machine platform image
VMSS2	- Orchestration mode: Uniform - Image type: Windows Server virtual machine custom image
VMSS3	- Orchestration mode: Flexible - Image type: Linux virtual machine platform image
VMSS4	- Orchestration mode: Uniform - Image type: Linux virtual machine custom image

You are evaluating Azure Update Manager and automatic virtual machine guest patching. Which virtual machine scale sets will automatic guest patching support?

- A. VMSS2 and VMSS4 only
- B. VMSS1 and VMSS3 only
- C. VMSS1 only
- D. VMSS2 only
- E. VMSS1, VMSS2, VMSS3, and VMSS4

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 22

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: ([SHOW ANSWER](#))

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.](https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels)

[microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels](https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels)

NEW QUESTION: 23

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 24

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 25

You have a Microsoft 365 subscription.

You configure Microsoft Purview Information Protection to apply sensitivity labels automatically.

You need to recommend a solution that will prevent users from uploading unlabeled files to Microsoft SharePoint Online if the files contain content defined by Microsoft Purview classifiers as sensitive.

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

Policy type:

- App control policy
- App protection policy
- compliance policy

Microsoft 365 service:

- Endpoint data loss prevention (EndPoint DLP)
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Purview insider risk management

Microsoft

Answer:

Answer Area

Policy type: App control policy
App protection policy
compliance policy

Microsoft 365 service: Endpoint data loss prevention (EndPoint DLP)
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Purview insider risk management

Explanation:

Answer Area

Policy type: Compliance policy

Microsoft 365 service: Endpoint data loss prevention (Endpoint DLP)

NEW QUESTION: 26

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

Security alert

2517569153524258480_f132eeba-b7c9-4942-bf62-d0dd52ccfe74

MicroBurst exploitation toolkit used to extract keys to your storage accounts
(Preview) [Sample alert](#)

High **Active** **02/20/22, 0...**
Severity Status Activity time

Alert description [Copy alert JSON](#)

THIS IS A SAMPLE ALERT: MicroBurst's exploitation toolkit was used to extract keys to your storage accounts. This was detected by analyzing Azure Activity logs and resource management operations in your subscription.

Affected resource

Azure Training Subscription

Alert details **Take action**

MicroBurst modules
Get-AZStorageKeysREST

Detected by
 Microsoft

PrincipalOid
00000000-0000-0000-0000-000000000000

IP address
00.00.00.000

Username
Sample user

Microsoft

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

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

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 27

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:

Answer Area

Microsoft

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

Explanation:

Answer Area

Microsoft

Azure Backup: Encryption by using platform-managed keys

Azure Storage: Immutable storage

NEW QUESTION: 28

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 Apps
- C. Microsoft Defender for Cloud
- D. Microsoft Sentinel

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

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

All on-premises Windows 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:

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

- A. the Azure Monitor agent
- B. resource-based role-based access control (RBAC)
- C. Microsoft Entra Conditional Access policies
- D. Windows Server event subscription

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 30

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

To automate vulnerability code scanning:

- ☒ GitHub Enterprise Cloud
- ☐ GitHub Enterprise Server
- ☐ GitHub Team

To automatically generate pull requests:

- ☒ Dependabot
- ☐ Codespaces
- ☐ Dependency Tracker

Answer:

Answer Area

To automate vulnerability code scanning:

To automatically generate pull requests:

Explanation:

Answer Area

To automate vulnerability code scanning:

To automatically generate pull requests:

NEW QUESTION: 31

You have a Microsoft Entra tenant named contoso.com. You have 30 Azure subscriptions that are linked to contoso.com. The tenant contains the management groups shown in the following table.

Name	Description
Mgmt1	Contains 15 subscriptions
Mgmt2	Contains 15 subscriptions

You need to design a governance solution to manage access to all the Azure Storage accounts across the subscriptions. The solution must meet the following requirements:

- * Use custom role-based access control (RBAQ to provide granular access to control plane and data plane operations.
- * Minimize administrative effort.

At which scope should you assign the roles, and what is the minimum number of assignments per role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Scope:

Minimum number of assignments:

Answer:

Answer Area

Scope:

Minimum number of assignments:

Explanation:

Answer Area

Scope:

Minimum number of assignments:

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (343 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

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: (SHOW ANSWER)

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

NEW QUESTION: 33

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 ([LEAVE A REPLY](#))

<https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan> This rapid modernization plan (RaMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

NEW QUESTION: 34

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 35

You plan to deploy an Azure API Management solution that will enable different groups of developers to access different sets of APIs at random times and rates.

You need to recommend the pricing tier that should be purchased and the scope at which the rate limit policies should be applied. The solution must meet the following requirements:

- * Ensure that each group of developers can access only specific sets of APIs.
- * Ensure that each set of APIs can be configured with specific rate limits.
- * Minimize development and administrative effort and costs.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

Pricing tier: Standard V2

Basic V2

Consumption

Standard V2

Scope: API

Product

Workspace

Answer:

Answer Area

Microsoft

Pricing tier: Standard V2

Basic V2

Consumption

Standard V2

Scope: API

Product

Workspace

Explanation:

Answer Area

Microsoft

Pricing tier: Standard V2

Scope: Product

NEW QUESTION: 36

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: ([SHOW ANSWER](#))

Topic 1, 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 DS) forest named Utvware.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 (SOAR) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOC) 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.

NEW QUESTION: 37

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: ([SHOW ANSWER](#))

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>

NEW QUESTION: 38

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. No

B. Yes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

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. both SharePoint Online and Exchange Online

C. Exchange Online only

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

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 ([LEAVE A REPLY](#))

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.

Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

NEW QUESTION: 41

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: ([SHOW ANSWER](#))

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

Given the landing zone requirements of

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

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

NEW QUESTION: 42

You have an Azure subscription that is linked to a Microsoft Entra tenant.

You plan to deploy an enterprise application named Appl. App1 requires LDAP to look up attributes related to Microsoft Entra users.

You need to recommend a solution to support the LDAP requirement.

What should you recommend?

- A.** Configure a Conditional Access policy that has a trusted network location.
- B.** Deploy Microsoft Entra Private Access.
- C.** Deploy Microsoft Entra Domain Services.
- D.** Implement pass-through authentication.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 43

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: ([SHOW ANSWER](#))

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide> You can use sensitivity labels to: Provide protection settings that include encryption and content markings.

For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as Salesforce, Box, or Dropbox, even if the third-party app or service does not read or support sensitivity labels.

NEW QUESTION: 44

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 45

You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named AKS1.

AKS1 hosts a Windows node pool named Pool1 and a Linux node pool named Pool2.

You are designing a pool update strategy for AKS1.

You need to recommend how often to replace the operating system images deployed to the nodes. The solution must meet the following requirements:

- * Minimize how long it takes to apply operating system updates once the updates are released.
- * Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

Pool1: Weekly Monthly Quarterly

Pool2: Weekly Monthly Quarterly

Answer:

Answer Area

Pool1: Weekly Monthly Quarterly

Pool2: Weekly Monthly Quarterly



Explanation:

Answer Area



Pool1: Monthly

Pool2: Weekly

NEW QUESTION: 46

You have a Microsoft 365 subscription.

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

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online.

SharePoint Online, and Teams in near-real-time (NRT) in response to the following Azure AD events:

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

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

- A. Azure AD Privileged Identity Management (PIM)
- B. Conditional Access
- C. a sign-in risk policy
- D. Azure AD Application Proxy
- E. continuous access evaluation

Answer: ([SHOW ANSWER](#))

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (**343 Q&As** Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

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

The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

You plan to deploy Azure virtual machines that will run Windows Server.

You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

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

NOTE: Each correct selection is worth one point.

Answer Area

EDR:

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

SOAR:

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

Answer:

Answer Area

EDR:

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

SOAR:

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

Explanation:

EDR: 

SOAR: 

For SOAR read this <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks> Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of Microsoft Defender. <https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?>

view=o365-worldwide

NEW QUESTION: 48

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 49

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: ([SHOW ANSWER](#))

NEW QUESTION: 50

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:

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

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

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>

NEW QUESTION: 51

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.

Actions	Answer Area
⋮ Create an Azure Backup vault.	
⋮ From RG1, create a resource lock.	
⋮ Create a Recovery Services vault.	
⋮ Enable vault immutability.	
⋮ Lock immutability for the vault.	

Answer:

ctions

Create an Azure Backup vault.

From RG1, create a resource lock.

Create a Recovery Services vault.

Enable vault immutability.

Lock immutability for the vault.

Answer Area

Create a Recovery Services vault.

Enable vault immutability.

Lock immutability for the vault.

Explanation:

Actions

Create an Azure Backup vault.

From RG1, create a resource lock.

Answer Area

1 Create a Recovery Services vault.

2 Enable vault immutability.

3 Lock immutability for the vault.

NEW QUESTION: 52

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: (SHOW ANSWER)

(<https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide>)

NEW QUESTION: 53

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: (SHOW ANSWER)

<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>

NEW QUESTION: 54

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled.

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

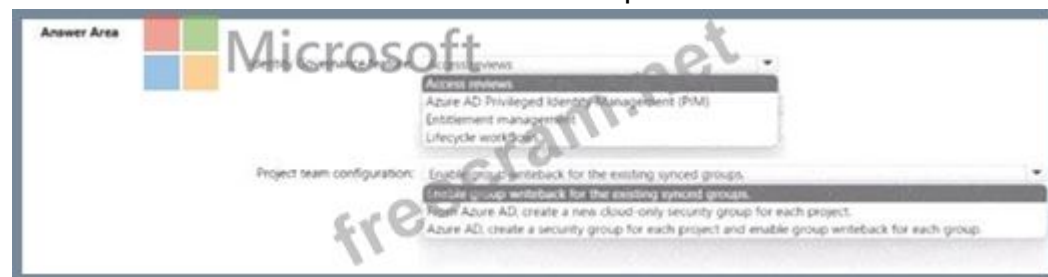
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD. Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

You need to recommend an Azure AD identity Governance solution that meets the following requirements:

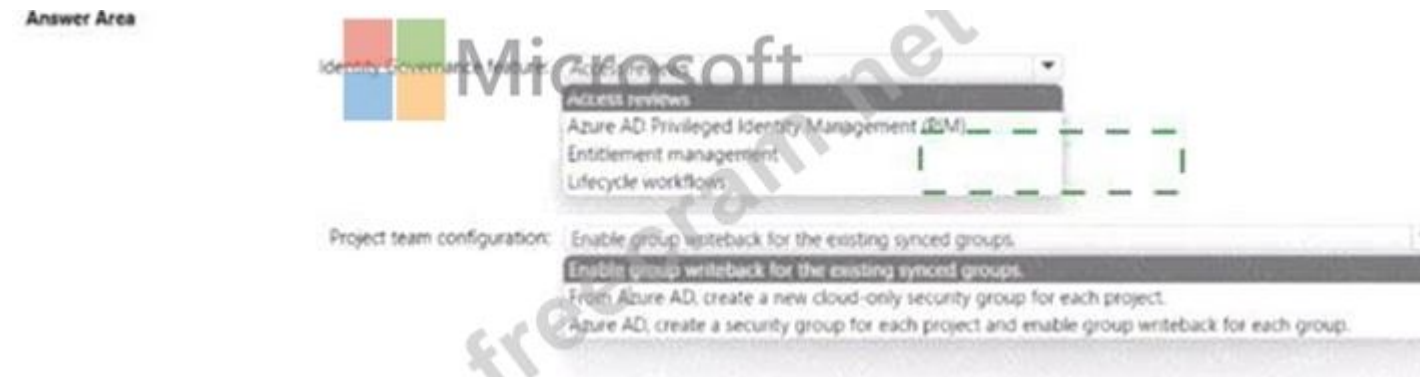
- * Project managers must verify that their project group contains only the current members of their project team.
- * The members of each project team must only have access to the resources of the project to which they are assigned.
- * Users must be removed from a project group automatically if the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

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 55

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. adaptive scopes

B. Azure AD Information Protection labels

C. administrative units

D. Microsoft 365 Defender user tags

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

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

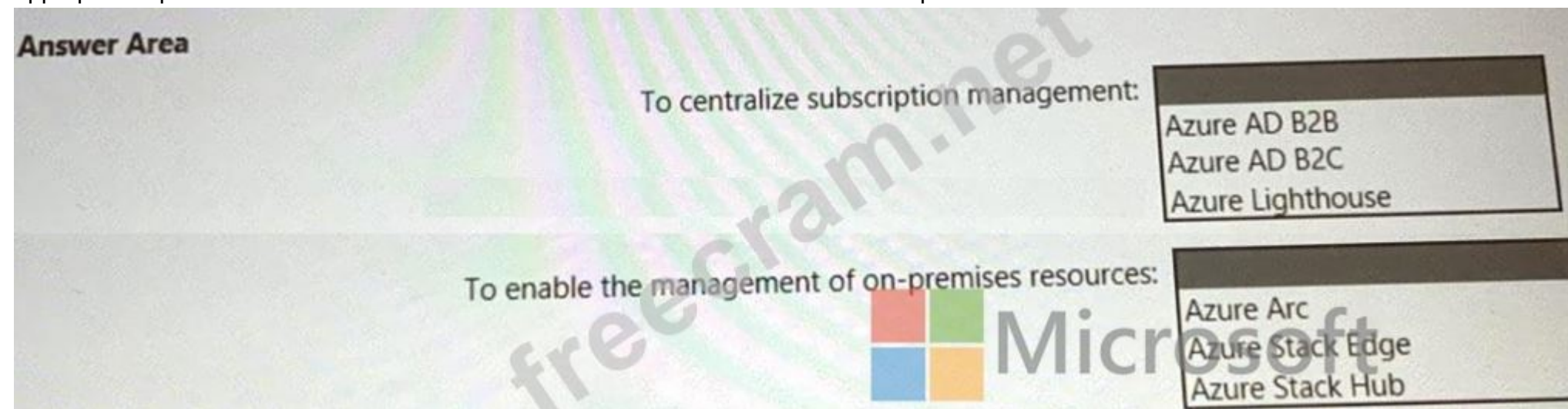
Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub



Answer:

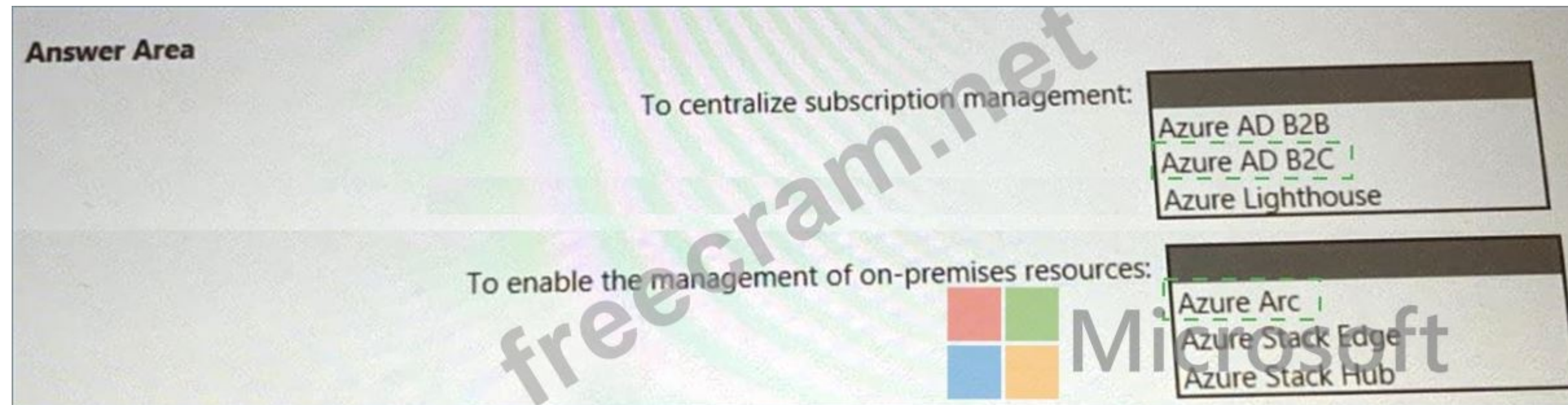
Answer Area

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub



Explanation:



NEW QUESTION: 57

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: (SHOW ANSWER)

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>

NEW QUESTION: 58

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 (LEAVE A REPLY)

(<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>)

<https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing?rtc=1>

NEW QUESTION: 59

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. Azure Advisor
- B. the Azure Well-Architected Framework
- C. Azure Security Benchmark v3
- D. the Azure landing zone accelerator

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 60

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 61

You have a Microsoft 365 E5 subscription.

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

- * Automatically identifies and stops external, brute force attacks against accounts in the subscription
 - * Automatically identifies and stops external attacks that use an internal account to exfiltrate data from Microsoft SharePoint Online sites in the subscription
- What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Automatically identifies and stops external, brute force attacks against accounts:



Automatically identifies and stops external attacks that use an internal account to exfiltrate data from SharePoint Online sites:



Answer:

Answer Area

Automatically identifies and stops external, brute force attacks against accounts:

- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Entra ID Identity Governance
- Microsoft Entra ID Protection

Automatically identifies and stops external attacks that use an internal account to exfiltrate data from SharePoint Online sites:

- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Entra ID Identity Governance
- Microsoft Entra ID Protection



Explanation:

Answer Area

Automatically identifies and stops external, brute force attacks against accounts: Microsoft Entra ID Protection

Automatically identifies and stops external attacks that use an internal account to exfiltrate data from SharePoint Online sites: Microsoft Defender for Cloud Apps

Microsoft

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (343 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

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

The New York City office contains an on-premises app named App1.

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 application proxy, deploy:

- Two connectors to the default connector group
- A connector to the default connector group and a connector to a new connector group
- Two 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

Microsoft

Answer:

Answer Area

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

To optimize the connection between the connector and App1, use:

Two connectors to the default connector group

A connector to the default connector group and a connector to a new connector group

Two connectors to the default connector group

Two new connector groups that each contain a new connector

ExpressRoute with Microsoft peering

ExpressRoute with Microsoft peering

ExpressRoute with Microsoft peering and the premium add-on

ExpressRoute with private peering

Explanation:

Answer Area

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

To optimize the connection between the connector and App1, use:

Two connectors to the default connector group

ExpressRoute with Microsoft peering

NEW QUESTION: 63

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. Assign regulatory compliance policies.
- B. Review the inventory.
- C. Enable Defender plans.
- D. Configure auto provisioning.
- E. Add a workflow automation.

Answer: (SHOW ANSWER)

NEW QUESTION: 64

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

D. Use the Azure Monitor agent with the multi-homing configuration.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 65

You have a Microsoft Entra tenant that is linked to a Microsoft 365 subscription and an Azure subscription.

The tenant contains service principals that are used to access applications in the Azure subscription.

You need to recommend a solution to detect risky sign-ins and other risky activities performed by the service principals in the tenant. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

Answer Area

Service:
License type:
Microsoft

Answer:

Answer Area

Service:
License type:
Microsoft

Explanation:

Answer Area

Service:
License type:
Microsoft

Topic 2, 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 Vnet1 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.

NEW QUESTION: 66

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

- * Microsoft SharePoint Online
- * Microsoft Exchange Online
- * Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Scopes

Files and emails

Groups and sites

Schematized data assets

Answer Area

SharePoint Online:

Scope

Microsoft Teams:

Scope

Exchange Online:

Scope

Answer:

Scopes

Files and emails

Groups and sites

Schematized data assets

Answer Area

SharePoint Online:

Groups and sites

Microsoft Teams:

Groups and sites

Exchange Online:

Files and emails

Explanation:

Box 1: Groups and sites

Box 2: Groups and sites

Box 3: Files and emails -

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide> Go to label scopes

NEW QUESTION: 67

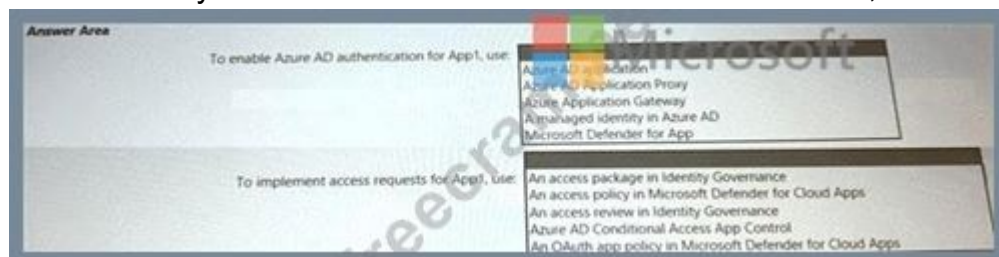
You are creating the security recommendations for an Azure App Service web app named App1.

App1 has the following specifications:

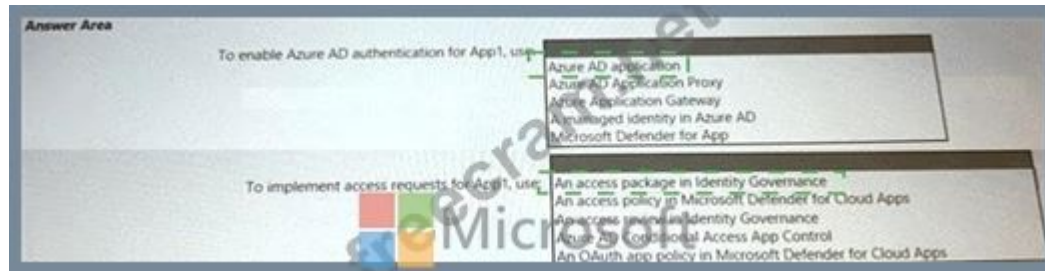
- * Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- * Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

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>

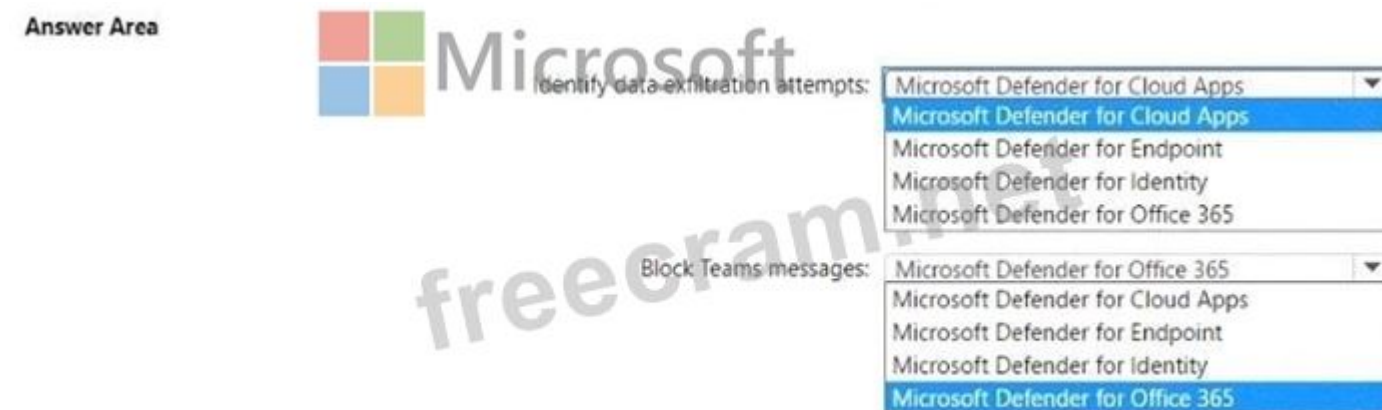
NEW QUESTION: 68

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:

Answer Area

Identify data exfiltration attempts:

Block Teams messages:

Explanation:

Answer Area

Identify data exfiltration attempts:

Block Teams messages:

NEW QUESTION: 69

You have a Microsoft 365 subscription that contains 1,000 users and a group named Group1. All the users have Windows 11 devices. The users sign in to their devices by using their Microsoft Entra account. The users do NOT have administrative rights to their devices.

The members of Group1 remotely assist the users by taking control of user sessions. The remote control sessions run in the security context of the users they are assisting.

You need to recommend a solution that will enable the Group1 members to run apps that require administrative rights to the users' devices. The solution must ensure that the apps are run in the context of each signed-in standard user.

What should you include in the recommendation?

- A. Privileged Identity Management (PIM) in Microsoft Entra ID
- B. Cloud Infrastructure Entitlement Management
- C. Windows Local Administrator Password Solution (Windows LAPS)
- D. Microsoft Intune Endpoint Privilege Management

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 70

You have on-premises servers and virtual machines that run Windows Server or Red Hat Enterprise Linux (RHEL).

You have an Azure subscription. The subscription contains virtual machines that run Windows Server Datacenter: Azure Edition.

You need to recommend a solution to manage operating system updates for the on-premises servers and the virtual machines. The solution must meet the following requirements:

- * Enable hotpatching for the Azure virtual machines.
- * Enable the on-demand inventory and deployment of updates.

* Enable the deployment of Extended Security Update (ESU) patches to the on-premises servers.
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

Microsoft

For update management, use:

- Azure Automanage
- Azure Update Manager
- System Center Updates Publisher

On the on-premises operating systems, install:

- Azure Monitor Agent
- The Azure Connected Machine agent
- Azure VPN client

Answer:

Answer Area

Microsoft

For update management, use:

- Azure Automanage
- Azure Update Manager
- System Center Updates Publisher

On the on-premises operating systems, install:

- Azure Monitor Agent
- The Azure Connected Machine agent
- Azure VPN client

Explanation:

Answer Area

Microsoft

For update management, use: Azure Update Manager

On the on-premises operating systems, install: The Azure Connected Machine agent

NEW QUESTION: 71

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:

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)

Explanation:

Evaluate regulatory compliance of cloud resources by assigning: Azure Policy initiatives to management groups

Evaluate regulatory compliance of on-premises resources by using: Azure Arc

NEW QUESTION: 72

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. Microsoft Defender for Cloud Apps
- D. SharePoint sites

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 73

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 74

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 75

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

 Microsoft

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

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

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

Answer:
Answer Area

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

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

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

Explanation:

Answer Area

 Microsoft

Role to assign to the Fabrikam helpdesk users for contoso.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

NEW QUESTION: 76

You have a Microsoft 365 subscription that contains 500 users. Each user is assigned a Microsoft 365 E5 license and uses a Windows device. Microsoft Purview data loss prevention (DLP) policies are applied to Microsoft Exchange Online email and SharePoint Online sites. You plan to monitor the usage of third-party generative AI apps by using Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

What should you do first?

- A.** Enable Microsoft Purview insider risk management for all the users.
- B.** Configure Microsoft Purview data connectors for the generative AI apps.
- C.** Onboard all endpoint devices to Microsoft Purview.
- D.** License all the users for Microsoft 365 Copilot.

Answer: ([SHOW ANSWER](#))

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (**343 Q&As** Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 77

You have an on-premises server named Server 1. Server1 is an FTP server that can be accessed by only the users at your company.

You have an Azure subscription.

You need to recommend a Zero Trust Network Access (ZTNA) solution to enforce Conditional Access policies when users access Server1 from the internet.

What should you include in the recommendation?

- A.** Azure Bastion
- B.** Microsoft Entra application proxy
- C.** Azure Application Gateway
- D.** Microsoft Entra Private Access
- E.** Microsoft Entra Internet Access

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 78

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

For the containers:

Blob	▼
Account	
Blob	
Container	

For the shares:

Account	▼
Account	
File	
Share	

Answer:

Answer Area



Microsoft

For the containers:

Blob	▼
Account	
Blob	
Container	

For the shares:

Account	▼
Account	
File	
Share	

Explanation:

Answer Area
For the containers: Blob ▼
For the shares: Account ▼

NEW QUESTION: 79

You have a Microsoft Sentinel deployment.

You are developing a solution to ensure that compliance with the MITRE ATT & CK framework is maintained as the framework evolves.

You need to recommend a solution to identify which MITRE ATT & CK techniques are NOT addressed by the current Microsoft Sentinel deployment. What should you include in the recommendation?

- A. the MITRE analytics explorer
- B. the MITRE coverage matrix
- C. the Microsoft Sentinel Analytics blade
- D. the Microsoft Sentinel Health Summary dashboard

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 80

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 Sentinel
- C. Microsoft Defender for Cloud
- D. Microsoft Defender for Cloud Apps

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 81

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 82

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:

Automated responses:

Microsoft

Answer:



Explanation:



NEW QUESTION: 83

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: [SHOW ANSWER](#)

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

NEW QUESTION: 84

You have a Microsoft Entra tenant that uses Microsoft Entra Private Access. You plan to publish a group of internal web apps by using a Global Secure Access application.

You need to ensure that users can access the web apps by connecting through the Global Secure Access application. What should you use?

A. a forwarding profile that directs all outbound internet traffic through the Microsoft backbone network

- B.** a Conditional Access policy that grants access from only compliant devices
- C.** an access policy that limits connections based on user groups
- D.** a connector group that contains the connectors used to access the web apps and a single endpoint for the internal fully qualified domain names (FQDNs)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 85

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.** app governance in Microsoft Defender for Cloud Apps
- B.** admin consent settings for enterprise applications in Azure AD
- C.** adaptive application controls in Defender for Servers
- D.** a compute policy in Azure Policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 86

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: ([SHOW ANSWER](#))

<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>

NEW QUESTION: 87

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

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

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

Actions

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

Answer Area

Navigation icons: > < ^ v

Answer:

Actions

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

Answer Area

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

Navigation icons: > < ^ v

Explanation:

Actions

- Establish ransomware recovery readiness.
- Implement disaster recovery.

Answer Area

- 1 Establish visibility.
- 2 Enable additional protection and detection controls.
- 3 Enable automation.

Navigation icons: > < ^ v

NEW QUESTION: 88

You have a Microsoft 365 subscription that contains 1,000 Microsoft Exchange Online mailboxes. You need to identify which users are susceptible to phishing attacks. What should you use?

- A. spoof intelligence insight in Exchange Online Protection (EOP)
- B. Attack simulation training in Microsoft Defender for Office 365
- C. user activity reports in Microsoft Purview insider risk management
- D. Attack path analysis in Microsoft Defender for Cloud

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 89

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 90

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: ([SHOW ANSWER](#))

<https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore>

NEW QUESTION: 91

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

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

Explanation:

Answer Area



Service: Microsoft Defender for Office 365

Policy type: Anti-phishing

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (343 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 92

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.

Methodologies

- Business continuity
- Data classification
- Just-in-time (JIT) access
- Segmenting access

Answer Area

Assume breach: Methodology

Verify explicitly: Methodology

Use least privilege access: Methodology

Answer:

Methodologies

- Business continuity
- Data classification
- Just-in-time (JIT) access
- Segmenting access

Answer Area

Assume breach: Segmenting access

Verify explicitly: Data classification

Use least privilege access: Just-in-time (JIT) access

Explanation:

Methodologies

- Business continuity
- Data classification
- Just-in-time (JIT) access
- Segmenting access

Answer Area

Assume breach: Segmenting access

Verify explicitly: Data classification

Use least privilege access: Just-in-time (JIT) access

NEW QUESTION: 93

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 94

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 ([LEAVE A REPLY](#))

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

NEW QUESTION: 95

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: ([SHOW ANSWER](#)**)**

The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image." <https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image>

NEW QUESTION: 96

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 97

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.** Configure Windows Local Administrator Password Solution (Windows LAPS) in legacy Microsoft LAPS emulation mode.
- B.** Only add Group2 to the local Administrators group.
- 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: ([SHOW ANSWER](#))

NEW QUESTION: 98

You have an Azure subscription. The subscription contains five Azure App Service instances that host public web apps. Each instance is deployed across three Azure regions.

The web apps handle sensitive customer data and must be protected from common web exploits and malicious bots.

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

- * Provides centralized management and updates for protection rules
- * Protects all the web apps without modifying the application code
- * Minimizes costs

What should you include in the recommendation?

- A.** Azure Firewall
- B.** Azure Application Gateway
- C.** Azure DDoS Protection
- D.** Azure Front Door

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 99

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: ([SHOW ANSWER](#))

<https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-enclaves>

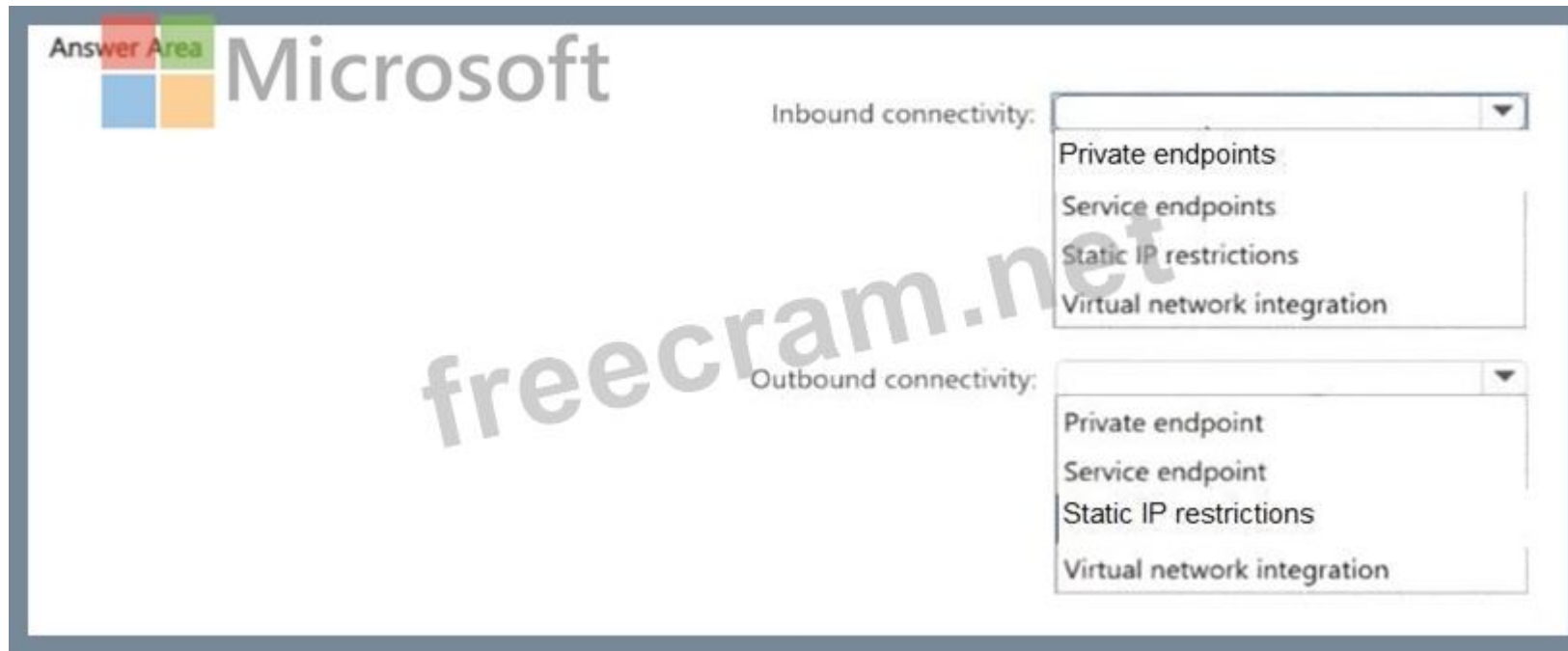
NEW QUESTION: 100

You have an Azure subscription that contains two virtual machines named VM1 and VM2 and an Azure App Service Standard web app named App1. VM1 is used to upload data to App1. App1 stores data on VM2.

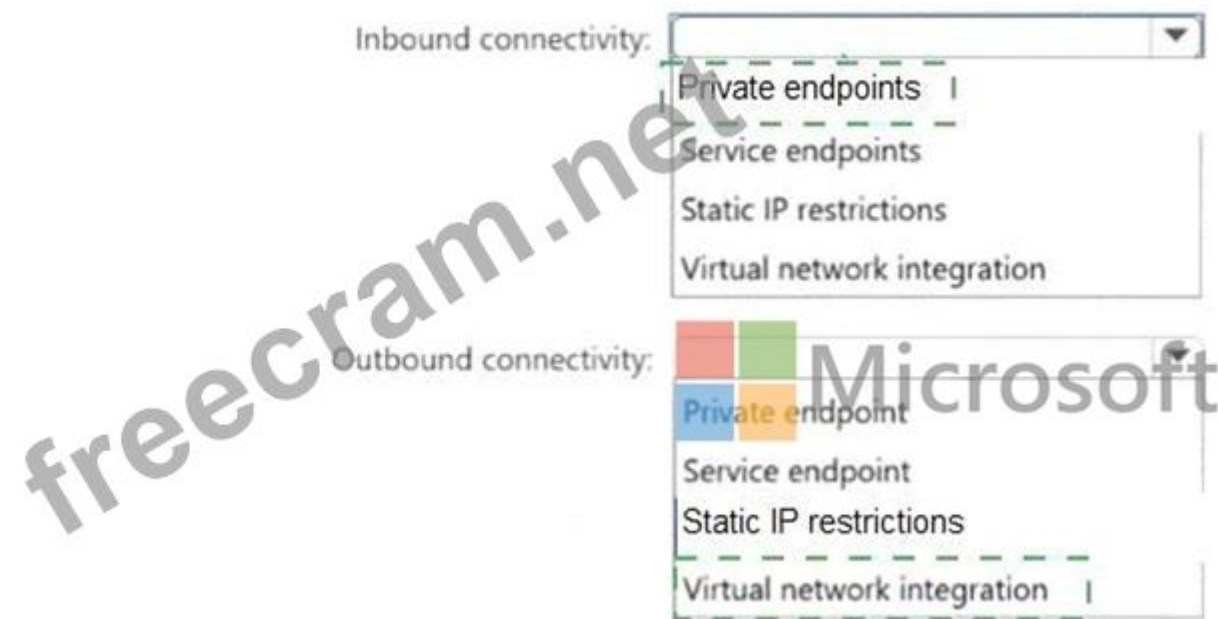
You need to secure connectivity between the virtual machines and App1. The solution must minimize the risk of data exfiltration.

What should you use to manage connectivity for App1? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.



Answer:
Answer Area



Explanation:



NEW QUESTION: 101

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. a managed identity in Azure
- D. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 102

You are designing a ransomware mitigation strategy

You perform a ransomware risk assessment and identify business-critical assets.

You need to recommend a solution to mitigate ransomware threats. The solution must follow Microsoft security best practices.

Which two actions should you include in the recommendation? Each correct answer presents a complete solution.

NOTE: Each correct answer is worth one point.

- A. Implement immutable, offline backups that have restricted access and test restore procedures regularly.
- B. Deploy Privileged Identity Management (PIM) that uses just-in-time (JIT) access and approval workflows.
- C. Enable firewall logging for auditing, without restricting inbound or outbound traffic.
- D. Use extended patching cycles to reduce the risk of update-related service disruptions.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 103

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 Profile1 that has a priority of 300 and contains a single web content filtering policy named WCFPolicy1 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.adatum.com:8433 will be blocked from all the devices.
- B. Traffic to https://www.fabrikam.com will be allowed from compliant devices only.
- C. Traffic to https://www.adatum.com:8433 will be allowed from all the devices.
- D. Traffic to https://www.fabrikam.com will be blocked from noncompliant devices only.
- E. Traffic to https://www.fabrikam.com will be allowed from all the devices.
- F. Traffic to https://www.adatum.com:8433 will be allowed from compliant devices only.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 104

You have an Azure subscription

You plan to deploy multiple containerized microservice-based apps to Azure Kubernetes 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.** Dapr
- B.** Envoy
- C.** Istio
- D.** Flux

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 105

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

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

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

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

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

Answer: ([SHOW ANSWER](#))

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

'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.' Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

NEW QUESTION: 106

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have Amazon Web Services (AWS), Google Cloud Platform (GCP). and Oracle Cloud Infrastructure (OCI) subscriptions.

You create a custom security standard in Defender for Cloud.

To which subscriptions can the Defender for Cloud standard be applied?

- A.** Azure, AWS, and GCP only
- B.** Azure, AWS. and OCI only
- C.** Azure and AWS only
- D.** Azure, AWS, GCP. and OCI

E. Azure and GCP only

Answer: ([SHOW ANSWER](#))

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (343 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 107

You have an Azure subscription that contains 15 custom apps. The source files for the apps are stored in Git repositories. The apps are deployed by using Azure DevOps.

You need to recommend a DevSecOps solution to implement static application security testing (SAST) of the app code to identify hard-coded secrets.

What should you include in the recommendation?

- A. Microsoft Dev Box
- B. Microsoft Defender for Key Vault
- C. Microsoft Defender for Cloud DevOps security
- D. GitHub Advanced Security

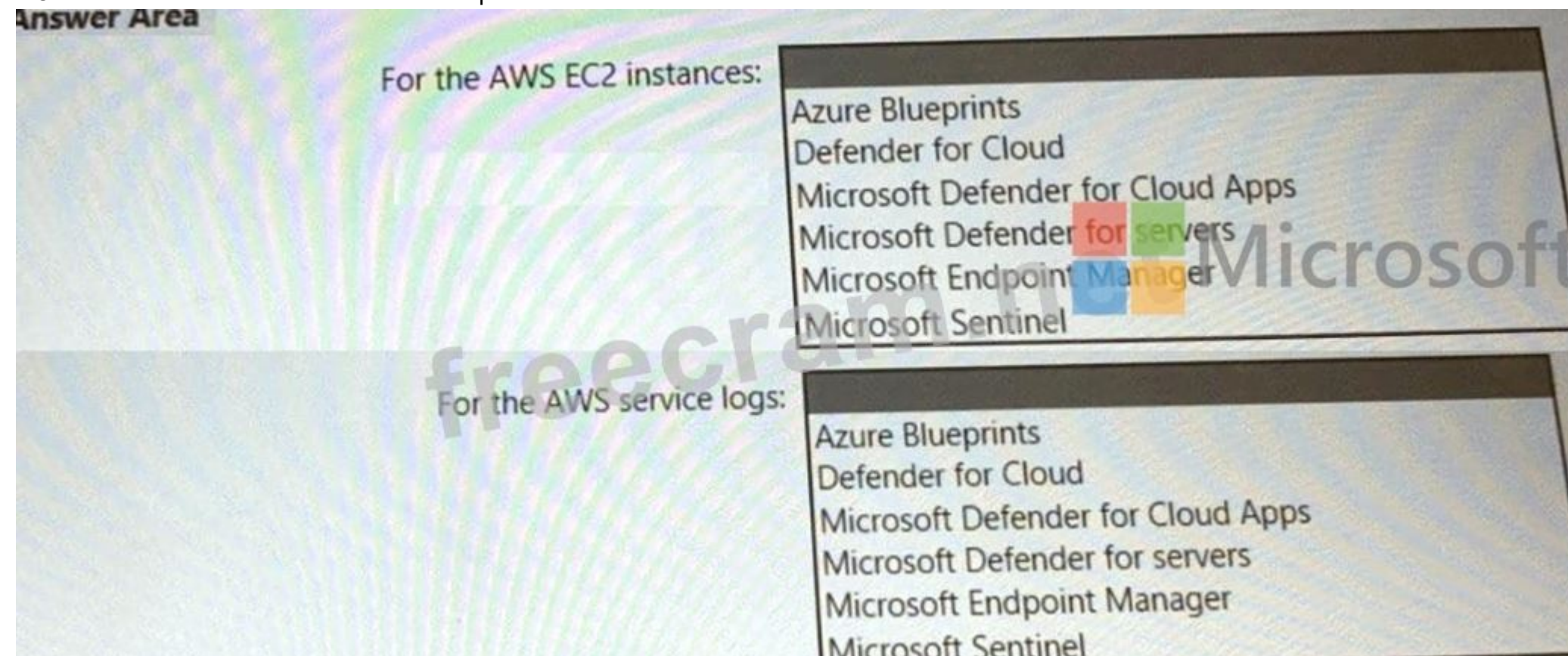
Answer: ([SHOW ANSWER](#))

NEW QUESTION: 108

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:

Answer Area

For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

Explanation:

For the AWS EC2 instances: Defender for Cloud

For the AWS service logs: Microsoft Sentinel

NEW QUESTION: 109

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 (LEAVE A REPLY)

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10>

NEW QUESTION: 110

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 111

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.

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

Answer:



NEW QUESTION: 112

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.** Azure SQL Database with virtualization-based security (VBS) enclaves
- B.** Azure SQL Managed Instance that has Always Encrypted configured
- C.** Azure SQL Database with Intel Software Guard Extensions (Intel SGX) enclaves
- D.** SQL Server on Azure Virtual Machines with virtualization-based security (VBS) enclaves

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 113

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

Account type for the developers:

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

Component in Identity Governance:

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

Answer:

Account type for the developers:

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

Component in Identity Governance:

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

Explanation:

Box 1: A synced user account -

Need to use a synced user account.

Box 2: An access review

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

NEW QUESTION: 114

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 115

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender. You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender. You need to recommend a solution to meet the following requirements:

- * Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
 - * Automatically generate incidents when the IP address of a command-and control server is detected in the events
- What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

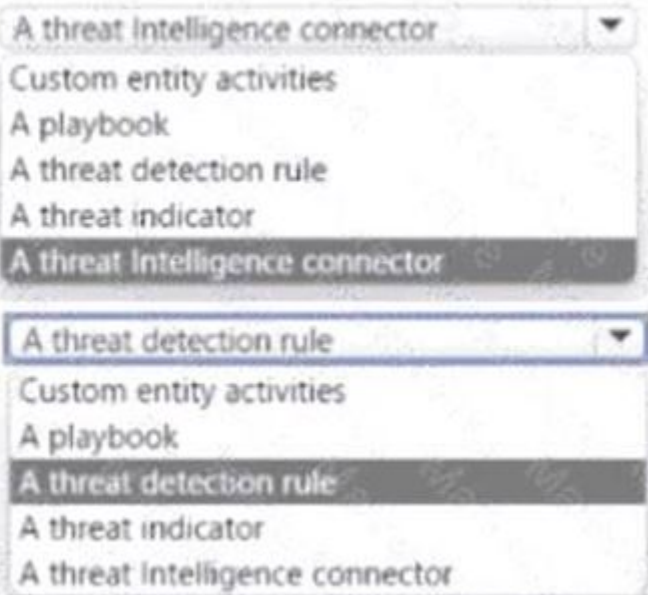
NOTE: Each correct selection is worth one point.

Answer Area

Integrate Microsoft Sentinel with a third-party security vendor:

Automatically generate incidents:

 Microsoft



Answer:

Answer Area

 Microsoft

Integrate Microsoft Sentinel with a third-party security vendor:

Automatically generate incidents:



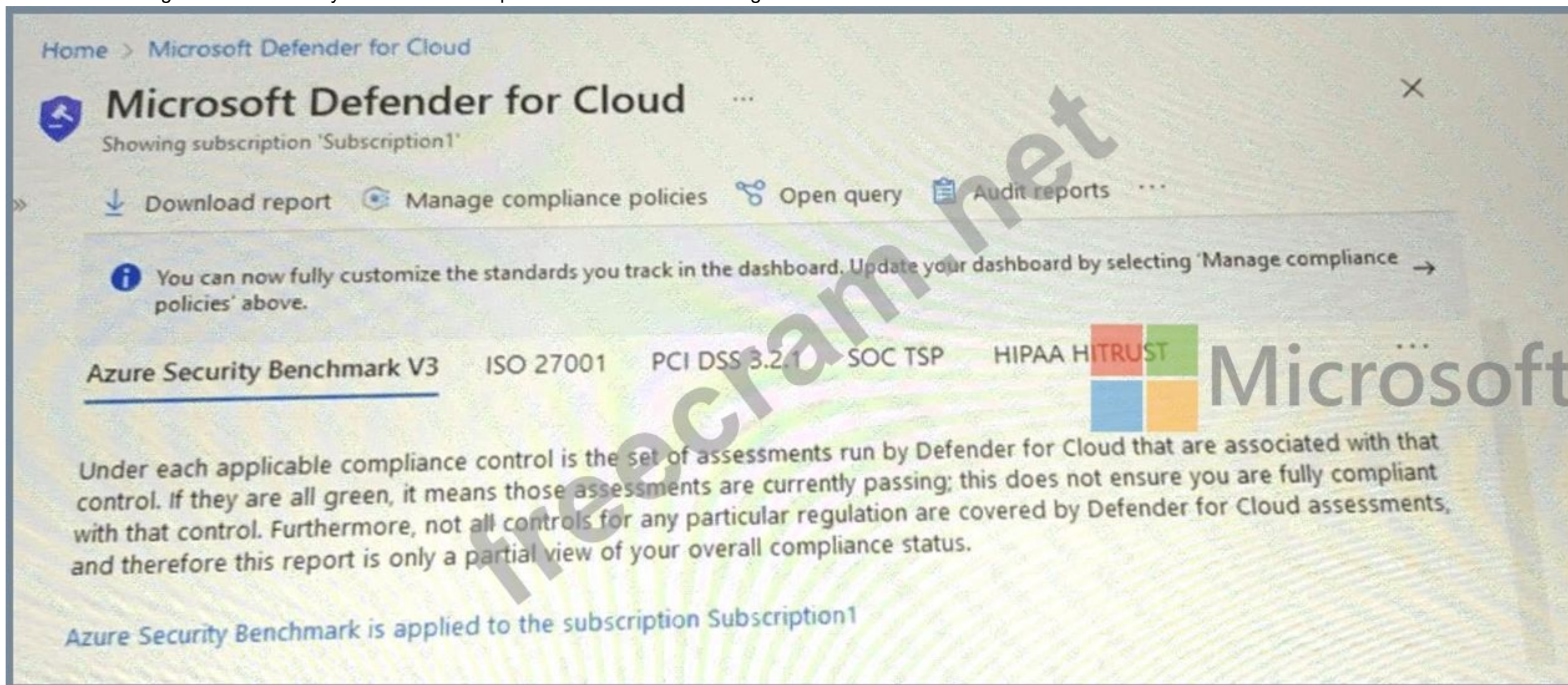
Explanation:

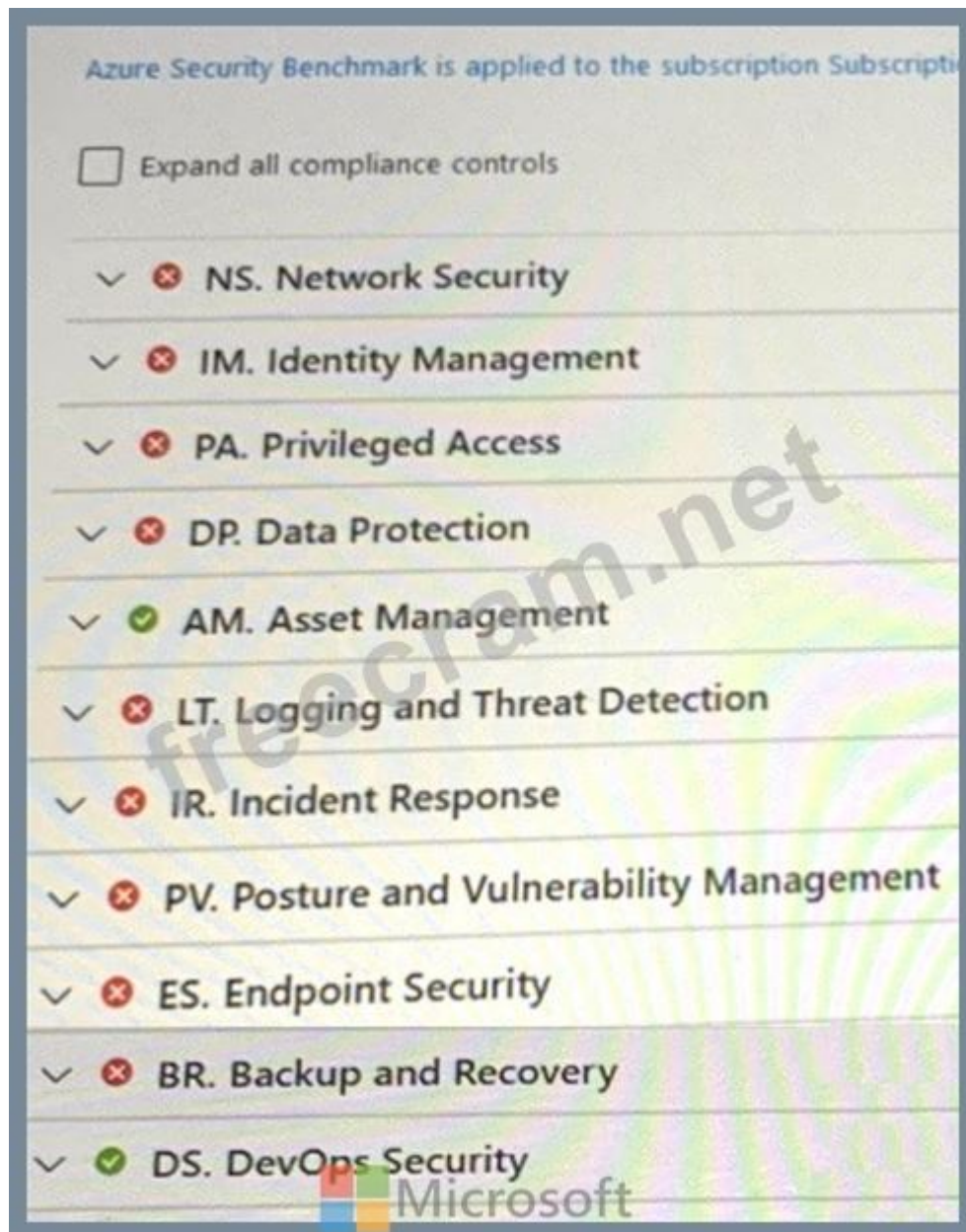


NEW QUESTION: 116

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

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.





You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

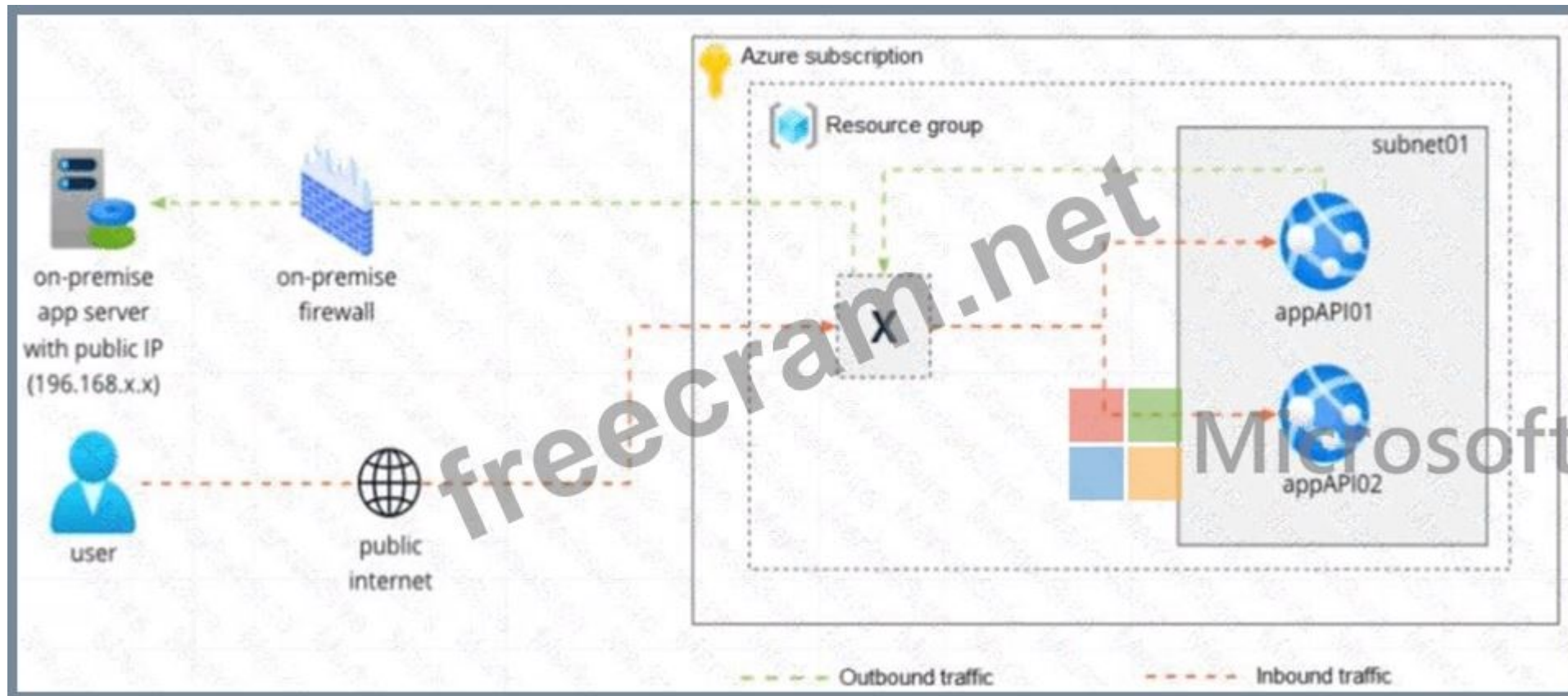
- A. Data Protection
- B. Incident Response
- C. Posture and Vulnerability Management
- D. Asset Management
- E. Endpoint Security

Answer: ([SHOW ANSWER](#))

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security>

NEW QUESTION: 117

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 on-premises 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: (SHOW ANSWER)

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

NEW QUESTION: 118

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: (SHOW ANSWER)

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

NEW 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. Enable threat detection for identity and access management.
- B. Use a centralized identity and authentication system.
- C. Protect identity and authentication systems.
- D. Manage the lifecycle of identities and entitlements
- E. Manage application identities securely and automatically.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 120

You have a Microsoft Entra tenant that uses Microsoft Entra ID Governance.

For each department in your company, you create a dedicated catalog and access packages to manage access to applications and data resources.

You need to ensure that team leaders in each department can perform the following actions:

- * Add or remove access package assignments for the users in their department
- * Prevent the access packages from appearing in each user ' s My Access portal.

The solution must follow the principle of least privilege. Which role should you assign to the team leaders?

- A. Catalog Owner
- B. Access Package Manager
- C. Access Package Assignment Manager
- D. Identity Governance Administrator

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 121

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 in Defender for Cloud
- D. app protection policies in Microsoft Endpoint Manager

Answer: ([SHOW ANSWER](#))

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

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (**343** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 122

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 123

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: ([SHOW ANSWER](#))

<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>

NEW QUESTION: 124

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 Sync. You need to monitor Domain1 for privilege escalation attacks. What should you use?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 125

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. BitLocker Drive Encryption (BitLocker)
- B. Azure Files
- C. protected folders
- D. Microsoft Defender for Endpoint
- E. Windows Defender Device Guard

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 126

You have a Microsoft 365 ES subscription. The subscription contains 500 devices that run Windows 11 Pro and are enrolled in Microsoft Intune You need to evaluate the use of Microsoft Defender Vulnerability Management to provide recommended configuration changes for the devices. Which Endpoint security settings should you use to review the recommended changes?

- A. Attack surface reduction
- B. Security tasks
- C. Device compliance
- D. Endpoint detection and response

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 127

You have an Azure subscription.
You need to create an Azure policy to ensure that all the resources in the subscription have tags assigned. The solution must ensure that the policy can remediate noncompliant resources automatically.
How should you configure the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Microsoft

Property to add:

conflictEffect

existenceCondition

roleDefinitionIds

Effect to use:

append

Modify

mutate

Answer:

Answer Area

Property to add:

Effect to use:

Microsoft

Explanation:

Answer Area

Property to add:

Effect to use:

Microsoft

NEW QUESTION: 128

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

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

NOTE: Each correct selection is worth one point

Answer Area

Threat modeling:

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

Actionable intelligence:



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

Dynamic application security testing (DAST):

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

Answer:

Answer Area



Threat modeling:

Actionable intelligence:

Dynamic application security testing (DAST):

Explanation:

Answer Area



Threat modeling:

Actionable intelligence:

Dynamic application security testing (DAST):

NEW QUESTION: 129

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 Entra entitlement management
- B. Endpoint Privilege Management (EPM)
- C. Privileged Identity Management (PIM)
- D. Microsoft Local Administrator Password Solution (Microsoft LAPS)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 130

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 Firewall
- C. Azure Front Door
- D. Azure Application Gateway

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 131

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. No
- B. Yes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 132

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. No
- B. Yes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 133

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 ([LEAVE A REPLY](#))

NEW QUESTION: 134

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

NOTE: Each correct selection is worth one point.

Answer Area

Infrastructure scanning:

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

Static application security testing:

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

Answer:

Answer Area

Infrastructure scanning:

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

Static application security testing:

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

Explanation:



NEW QUESTION: 135

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.

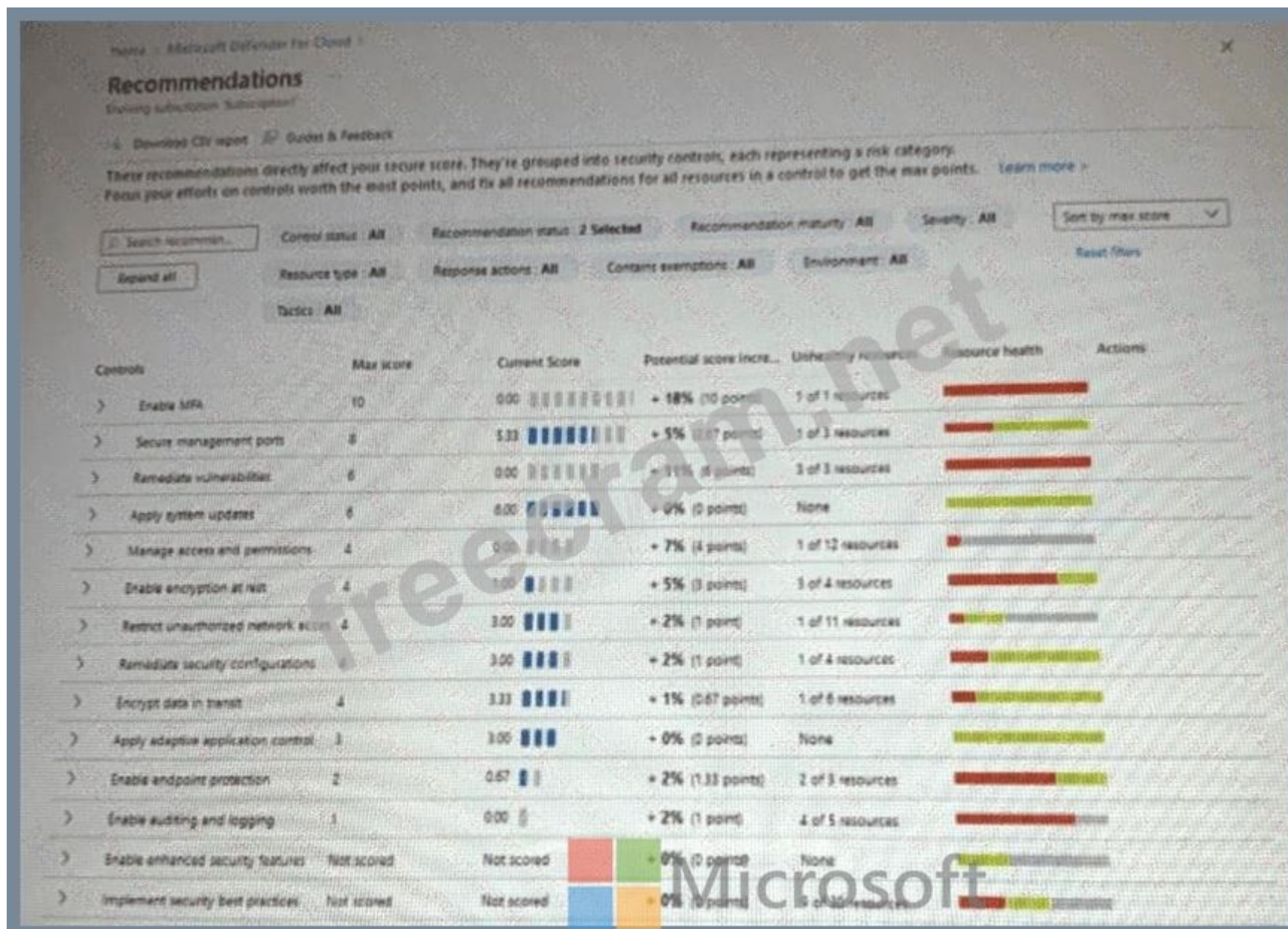
NOTE: Each correct answer is worth one point.

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 136

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

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

Answer:

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)

Microsoft

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

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

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>

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (343 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 137

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. Controlled folder access
- B. Windows Defender Device Guard
- C. Azure Files
- D. BitLocker Drive Encryption (BitLocker)
- E. Microsoft Defender for Endpoint

Answer: ([SHOW ANSWER](#))

Valid SC-100 Dumps shared by EduDump.com for Helping Passing SC-100 Exam! EduDump.com now offer the **newest SC-100 exam dumps**, the EduDump.com SC-100 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-100 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-100/premium/> (343 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)