Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1
- (Exam Topic 3)
You have a Microsoft 365 subscription
You need to recommend a security solution to monitor the following activities:
• User accounts that were potentially compromised
• Users performing bulk file downloads from Microsoft SharePoint Online
What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each Correct selection is worth one Point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exf https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users
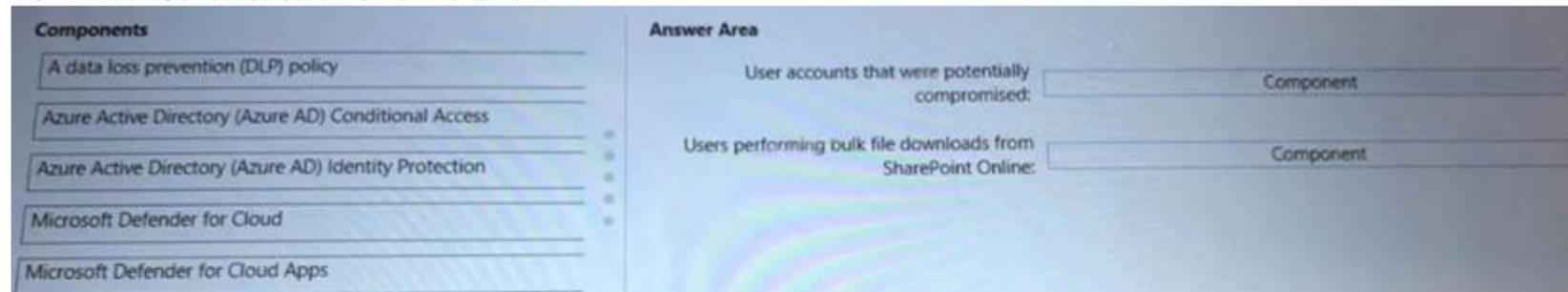
NEW QUESTION 2
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 3
- (Exam Topic 3)
Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment. You need to recommend the top three modernization areas to prioritize as part of the plan.
Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: ABD

NEW QUESTION 4
- (Exam Topic 3)
You are evaluating an Azure environment for compliance.
You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.
Which effect should you use in Azure Policy?

A. Deny
B. Disabled
C. Modify
D. Append

Answer: B

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

NEW QUESTION 5
- (Exam Topic 3)
Your company has the virtual machine infrastructure shown in the following table.

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

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure. You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks
such as ransomware.
What should you include in the recommendation?

A. Use geo-redundant storage (GRS).
B. Use customer-managed keys (CMKs) for encryption.
C. Require PINs to disable backups.
D. Implement Azure Site Recovery replication.

Answer: C

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

NEW QUESTION 6
- (Exam Topic 3)
Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.
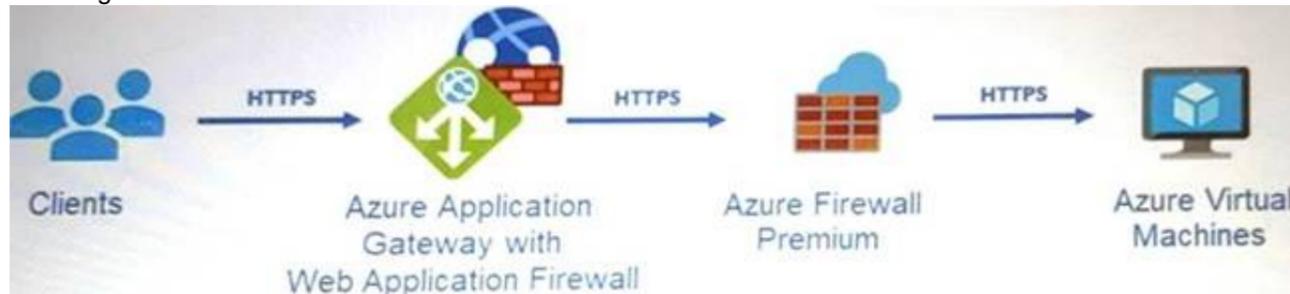
You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.
• Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
• Use Defender for Cloud to review alerts from the virtual machines.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 7
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation.
You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: BDE

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

NEW QUESTION 8
- (Exam Topic 3)
You have a Microsoft 365 subscription.
You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated
users on unmanaged devices.
Which two services should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 9
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload
protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What
should you include in the recommendation?

A. Azure Monitor webhooks
B. Azure Logics Apps
C. Azure Event Hubs
D. Azure Functions apps

Answer: B

Explanation:
The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory
compliance.Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems.
With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

NEW QUESTION 10
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware
attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one
point.

A. Azure Active Directory (Azure AD) Conditional Access policies
B. a custom collector that uses the Log Analytics agent
C. resource-based role-based access control (RBAC)
D. the Azure Monitor agent

Answer: CD

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

NEW QUESTION 10
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are
configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure. You plan to deploy Azure virtual machines that will run Windows Server.
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.
How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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

SOAR:
- Configure Microsoft Sentinel analytics rules.
- Configure Microsoft Sentinel playbooks.
- Configure regulatory compliance standards in Defender for Cloud.
- Configure workflow automation in Defender for Cloud.
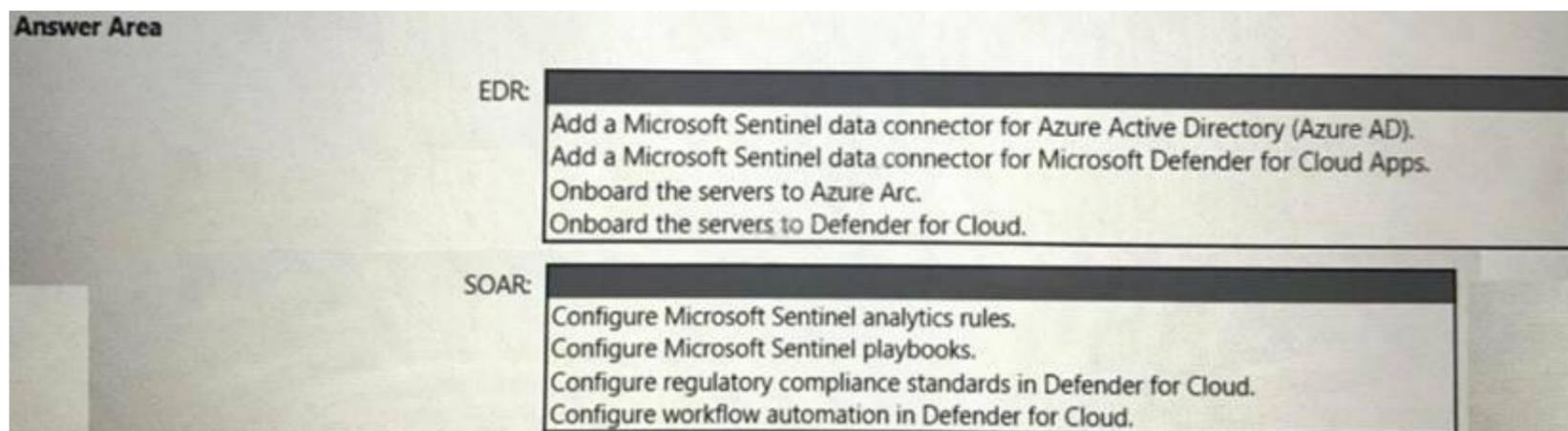
A. Mastered
B. Not Mastered

Answer: A

Explanation:
For SOAR read this https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of
Microsoft Defender.
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

NEW QUESTION 12
- (Exam Topic 3)
You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers.
In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: AC

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

NEW QUESTION 13
- (Exam Topic 3)
You are designing a ransomware response plan that follows Microsoft Security Best Practices.
You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files. What should you include in the recommendation?

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

Answer: E

NEW QUESTION 18
- (Exam Topic 3)
Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

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

Answer: AB

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

NEW QUESTION 19
- (Exam Topic 3)
You are designing the security standards for a new Azure environment.
You need to design a privileged identity strategy based on the Zero Trust model. Which framework should you follow to create the design?

A. Enhanced Security Admin Environment (ESAE)
B. Microsoft Security Development Lifecycle (SDL)
C. Rapid Modernization Plan (RaMP)
D. Microsoft Operational Security Assurance (OSA)

Answer: C

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

NEW QUESTION 20
- (Exam Topic 3)
You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AO credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

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

Answer: A

NEW QUESTION 23
- (Exam Topic 3)
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.
What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: ACE

NEW QUESTION 26
- (Exam Topic 3)
You are designing the security architecture for a cloud-only environment.
You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).
You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:
• Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
• Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.
What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

DLP: Microsoft Purview ▼
Azure Data Catalog
Azure Data Explorer
Microsoft Purview

UEBA: Azure AD Identity Protection ▼
Azure AD Identity Protection
Microsoft Defender for Identity
Microsoft Entra Verified ID

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

DLP: Microsoft Purview ▼
Azure Data Catalog
Azure Data Explorer
Microsoft Purview

UEBA: Azure AD Identity Protection ▼
Azure AD Identity Protection
Microsoft Defender for Identity
Microsoft Entra Verified ID

NEW QUESTION 30
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/sele

NEW QUESTION 33
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 38
- (Exam Topic 3)
You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

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

Answer: D

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-w

NEW QUESTION 39
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, review the secure score recommendations.
C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
D. From Defender for Cloud, enable Defender for Cloud plans.

Answer: C

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

NEW QUESTION 42
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
• Ensure that only authorized applications can run on the kiosks.
• Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard the kiosks to Azure Monitor.
B. Implement Privileged Access Workstation (PAW) for the kiosks.
C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Answer: DE

Explanation:
(https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerab

NEW QUESTION 43
- (Exam Topic 2)
You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Evaluate regulatory compliance of cloud resources by assigning:	Azure Policy definitions to management groups
	Azure Policy initiatives to management groups
	Azure Policy initiatives to subscriptions
Evaluate regulatory compliance of on-premises resources by using:	Azure Arc
	Group Policy
	PowerShell Desired State Configuration (DSC)

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Evaluate regulatory compliance of cloud resources by assigning:	Azure Policy definitions to management groups
	Azure Policy initiatives to management groups
	Azure Policy initiatives to subscriptions
Evaluate regulatory compliance of on-premises resources by using:	Azure Arc
	Group Policy
	PowerShell Desired State Configuration (DSC)

NEW QUESTION 47
- (Exam Topic 2)
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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 50
- (Exam Topic 1)
You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?

A. Azure Key Vault

B. GitHub Advanced Security
C. Application Insights in Azure Monitor
D. Azure DevTest Labs

Answer: B

Explanation:

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

NEW QUESTION 53
- (Exam Topic 1)
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: AC

Explanation:

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

NEW QUESTION 58
- (Exam Topic 1)
You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

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

Answer: A

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

NEW QUESTION 61
- (Exam Topic 1)
You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements. What should you include in the recommendation?

A. Transparent Data Encryption (TDE)
B. Always Encrypted
C. row-level security (RLS)
D. dynamic data masking
E. data classification

Answer: D

Explanation:

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

NEW QUESTION 66
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend configuring gateway-required virtual network integration. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 67
- (Exam Topic 3)
Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies
B. Azure AD workbooks to monitor risk detections
C. custom resource owner password credentials (ROPC) flows in Azure AD B2C

D. access packages in Identity Governance
E. smart account lockout in Azure AD B2C

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

NEW QUESTION 70
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically
What should you use?

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

Answer: B

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

NEW QUESTION 74
- (Exam Topic 3)
You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using
continuous integration and continuous deployment (CI/CD) pipelines.
You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.
What should you recommend?

A. an Azure AD user account that has a password stored in Azure Key Vault
B. a group managed service account (gMSA)
C. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management{PIM}
D. a managed identity in Azure

Answer: D

NEW QUESTION 76
- (Exam Topic 3)
Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled.
You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.
You need to recommend an Azure AD identity Governance solution that meets the following requirements:
• Project managers must verify that their project group contains only the current members of their project team
• The members of each project team must only have access to the resources of the project to which they are assigned
• Users must be removed from a project group automatically if the project manager has MOT verified the group s membership for 30 days.
• Administrative effort must be minimized.
What should you include in the recommendation? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area
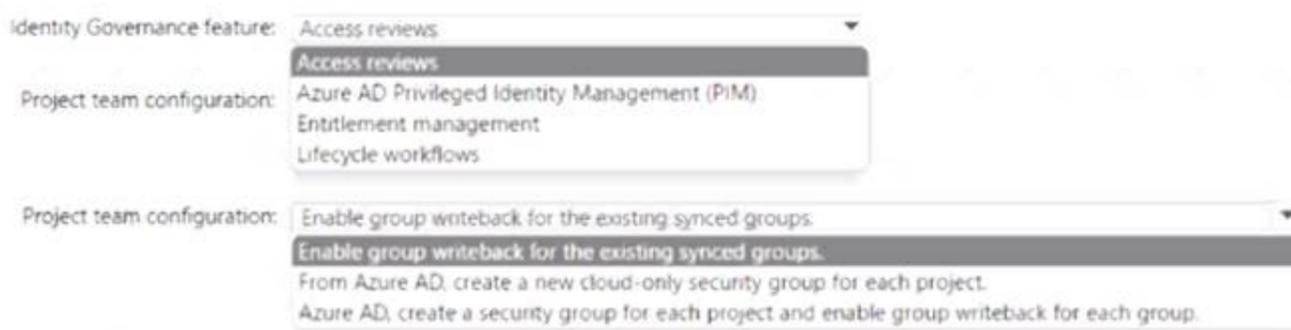
Identity Governance feature: Access reviews ▼
                                Access reviews
Project team configuration: Azure AD Privileged Identity Management (PIM)
                                Entitlement management
                                Lifecycle workflows

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Identity Governance feature: | Access reviews | ▼ |

| Access reviews |
| Azure AD Privileged Identity Management (PIM) |
| Entitlement management |
| Lifecycle workflows |

Project team configuration:

Project team configuration: | Enable group writeback for the existing synced groups. | ▼ |

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

NEW QUESTION 79
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 82
- (Exam Topic 3)
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.
You need to recommend a solution for the customer. The solution must minimize costs. What should you include in the recommendation?

A. Microsoft 365 Defender
B. Microsoft Defender for Cloud
C. Microsoft Defender for Cloud Apps
D. Microsoft Sentinel

Answer: D

NEW QUESTION 84
- (Exam Topic 3)
You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:
• Prevent the need to enable ports 3389 and 22 from the internet.
• Only provide permission to connect the virtual machines when required.
• Ensure that administrators use the Azure portal to connect to the virtual machines.
Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: DE

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

NEW QUESTION 87
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:
• Windows 11 devices managed by Microsoft Intune
• Azure Storage accounts
• Azure virtual machines
What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

Windows 11 devices:

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

Azure virtual machines:

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

Azure Storage accounts:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it). Selection 2: Microsoft Defender for Cloud.
Selection 3: Microsoft Defender for Cloud.
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-sec

NEW QUESTION 89
- (Exam Topic 3)
Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.
You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.
You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.
What should you include in the recommendation?

A. custom roles in Azure Pipelines
B. branch policies in Azure Repos
C. Azure policies
D. custom Azure roles

Answer: B

NEW QUESTION 93
- (Exam Topic 3)
You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender
You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender
You need to recommend a solution to meet the following requirements:
• Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
• Automatically generate incidents when the IP address of a command-and control server is detected in the events
What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Integrate Microsoft Sentinel with a third-party security vendor:

A threat intelligence connector ▼
Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat Intelligence connector

Automatically generate incidents:

A threat detection rule ▼
Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat Intelligence connector

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat Intelligence connector

Automatically generate incidents: | A threat detection rule | ▼

Custom entity activities
A playbook
A threat detection rule
A threat indicator
A threat Intelligence connector

NEW QUESTION 97
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.
The company's security policy prevents the use of personal devices for accessing company data and applications.
You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.
What should you include in the recommendation?

A. Migrate the on-premises applications to cloud-based applications.
B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

Answer: D

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

---

NEW QUESTION 98
- (Exam Topic 3)
For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management What should you include in the recommendation?

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

Answer: E

NEW QUESTION 103
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance. What should you do first?

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

Answer: D

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

---

NEW QUESTION 104
- (Exam Topic 3)
Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks. The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:

• Prevent exposing the public IP addresses of the virtual machines.
• Provide the ability to connect without using a VPN.
• Minimize costs.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AD

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

NEW QUESTION 106
- (Exam Topic 3)
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux. You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:
• Identify missing updates and insecure configurations.
• Use the Qualys engine. What should you use?

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

Answer: A

NEW QUESTION 109
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

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

Answer: B

NEW QUESTION 111
- (Exam Topic 3)
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 Area

App1:
App2:
Azure AD B2B authentication with Conditional Access
Azure AD B2C custom policies with Conditional Access
Azure Application Gateway Web Application Firewall policies
Azure Firewall
Azure VPN Gateway with network security group rules
Azure VPN Point-to-Site connections

App2:
Azure AD B2B authentication with Conditional Access
Azure AD B2C custom policies with Conditional Access
Azure Application Gateway Web Application Firewall policies
Azure Firewall
Azure VPN Gateway with network security group rules
Azure VPN Point-to-Site connections

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence

NEW QUESTION 116
- (Exam Topic 3)
You have an Azure SQL database named DB1 that contains customer information. A team of database administrators has full access to DB1.
To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information.
You need to design a security strategy for D81. The solution must meet the following requirements:
• When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.
• When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.
What should you include in the design? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

For the database administrators:
- Always Encrypted
- **Always Encrypted**
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators:
- Row-level security (RLS)
- Always Encrypted
- Dynamic data masking
- **Row-level security (RLS)**
- Transparent Data Encryption (TDE)

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

For the database administrators:
- Always Encrypted
- **Always Encrypted**
- Dynamic data masking
- Row-level security (RLS)
- Transparent Data Encryption (TDE)

For the operators:
- Row-level security (RLS)
- Always Encrypted
- Dynamic data masking
- **Row-level security (RLS)**
- Transparent Data Encryption (TDE)

NEW QUESTION 118
- (Exam Topic 3)
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 Cloud**
- GitHub Enterprise Server
- GitHub Team

To automatically generate pull requests:
- Dependabot
- Codespaces
- **Dependabot**
- Dependency Tracker

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A close up of a text Description automatically generated

NEW QUESTION 122
- (Exam Topic 3)
You are designing a security operations strategy based on the Zero Trust framework.
You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts. What should you do?

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

Answer: C

NEW QUESTION 123
- (Exam Topic 3)
You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).
You need to define the recovery steps for a ransomware attack that encrypted data in the subscription The solution must follow Microsoft Security Best Practices.
What is the first step in the recovery plan?

A. Disable Microsoft OneDnve sync and Exchange ActiveSync.
B. Recover files to a cleaned computer or device.
C. Contact law enforcement.
D. From Microsoft Defender for Endpoint perform a security scan.

Answer: A

NEW QUESTION 126
- (Exam Topic 3)
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.
B. Assign a policy to each subscription.
C. Assign a policy to a management group.
D. Assign an initiative to each subscription.
E. Assign a blueprint to each subscription.
F. Assign a blueprint to a management group.

Answer: AF

Explanation:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

NEW QUESTION 128
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 132
- (Exam Topic 3)
You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.
All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware 'You need to recommend which CONTROLS must be

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

NEW QUESTION 134
- (Exam Topic 3)
You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts. You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts. Which two configurations should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enable Microsoft Defender for Cosmos DB.
B. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.
C. Disable local authentication for Azure Cosmos DB.
D. Enable Microsoft Defender for Identity.
E. Send the Azure Cosmos DB logs to a Log Analytics workspace.

Answer: BC

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

NEW QUESTION 139
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SC-100 Practice Exam Features:

* SC-100 Questions and Answers Updated Frequently

* SC-100 Practice Questions Verified by Expert Senior Certified Staff

* SC-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SC-100 Practice Test Here