

# Microsoft

## Exam Questions SC-100

Microsoft Cybersecurity Architect



NEW QUESTION 1

- (Exam Topic 1)

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

- A. Mastered
- B. Not Mastered

Answer: A

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 2

- (Exam Topic 1)

You need to recommend a solution to meet the compliance requirements.

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

Answer Area

To enforce compliance to the regulatory standard, create:

An Azure Automation account

A blueprint

A managed identity

Workflow automation

To exclude TestRG from the compliance assessment:

Edit an Azure blueprint

Modify a Defender for Cloud workflow automation

Modify an Azure policy definition

Update an Azure policy assignment

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with> <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure>

while it is in policy assignment

- <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure>

NEW QUESTION 3

- (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: AD

**Explanation:**

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

**NEW QUESTION 4**

- (Exam Topic 1)

You need to recommend a solution to meet the AWS requirements.

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

**Answer Area**

For the AWS EC2 instances:

- 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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**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

**NEW QUESTION 5**

- (Exam Topic 2)

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

What should you configure for each landing zone?

- A. Azure DDoS Protection Standard
- B. an Azure Private DNS zone
- C. Microsoft Defender for Cloud
- D. an ExpressRoute gateway

**Answer:** D

**Explanation:**

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

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

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

**NEW QUESTION 6**

- (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

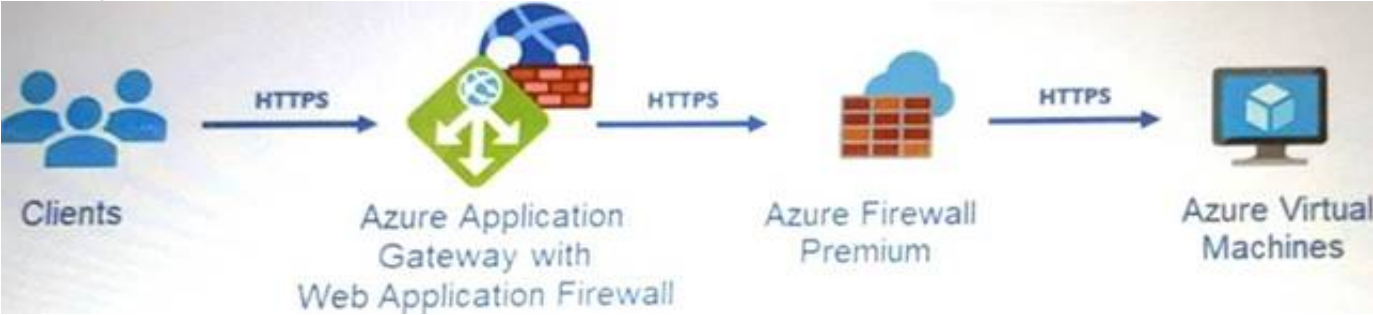
To ensure that you can perform leaked credential detection:

- 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 7**

- (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.

**Answer Area**

For WAF:

- The Azure Diagnostics extension
- Azure Network Watcher
- Data connectors
- Workflow automation

For the virtual machines:

- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- The Log Analytics agent
- Workflow automation

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface Description automatically generated

**NEW QUESTION 8**

- (Exam Topic 3)

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

You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out.

What should you include in the recommendations?

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

Answer: B

NEW QUESTION 9

- (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.

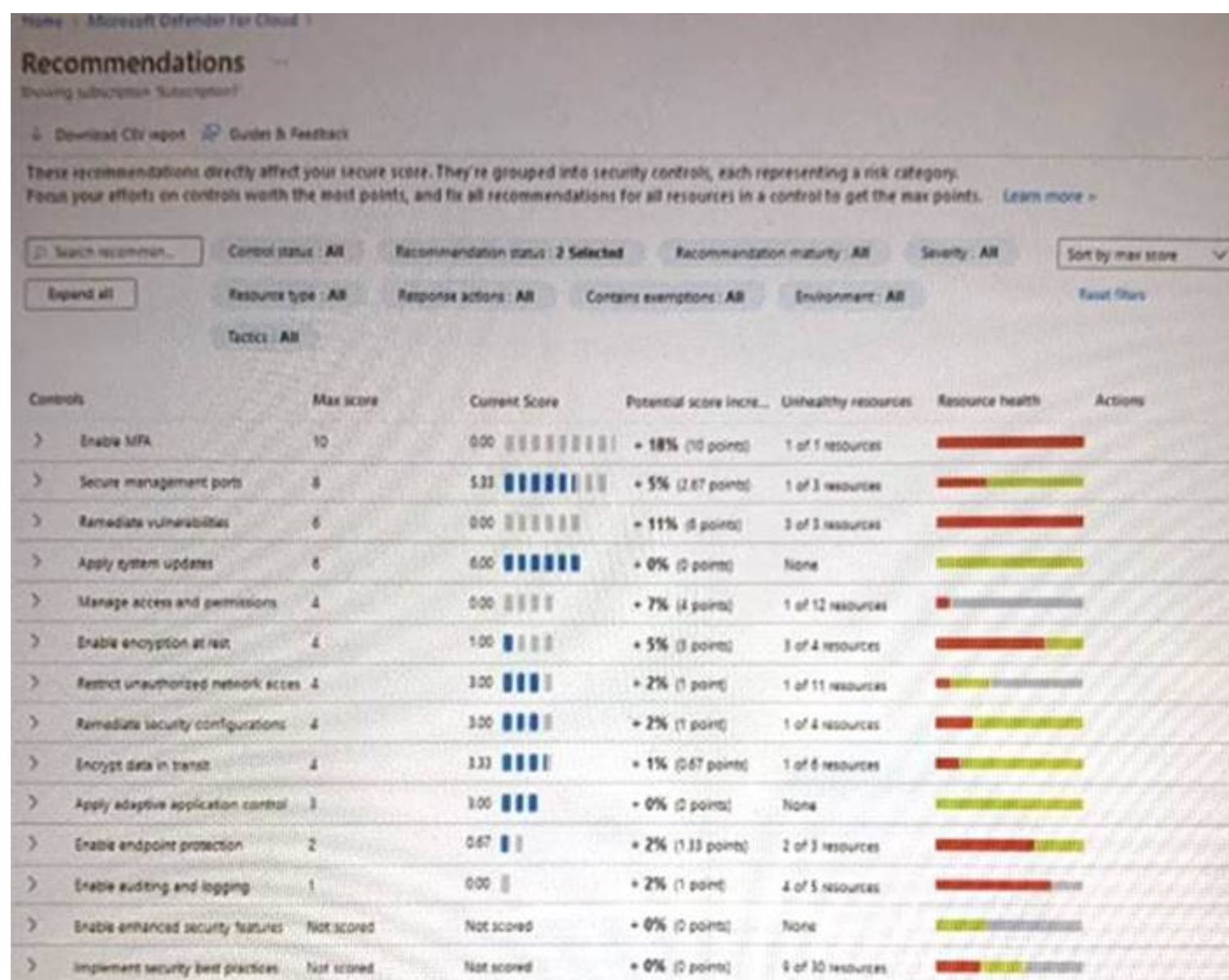
<https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-sec>

NEW QUESTION 10

- (Exam Topic 3)

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





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

**Answer Area**

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 10**

- (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 15

- (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 19

- (Exam Topic 3)

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

- A. service tags in network security groups (NSGs)
- B. managed rule sets in Azure Web Application Firewall (WAF) policies
- C. inbound rules in network security groups (NSGs)
- D. firewall rules for the storage account
- E. inbound rules in Azure Firewall

**Answer:** D

#### NEW QUESTION 24

- (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?

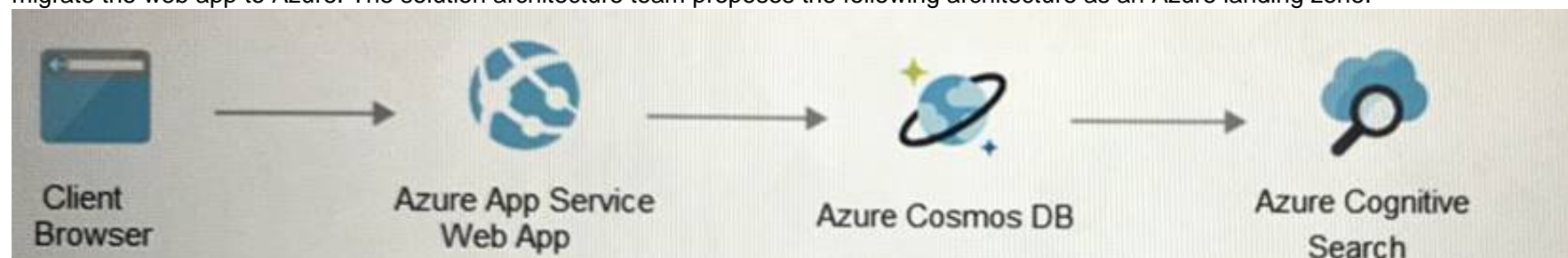
- A. data classification content explorer
- B. data loss prevention (DLP)
- C. eDiscovery
- D. Information Governance

**Answer:** B

#### NEW QUESTION 25

- (Exam Topic 3)

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



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

Solution: You recommend creating private endpoints for the web app and the database layer. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

#### Explanation:

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

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>

#### NEW QUESTION 29

- (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 34**

- (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 36**

- (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 41**

- (Exam Topic 3)

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).

You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment

What should you include during the application design phase?

- A. static application security testing (SAST) by using SonarQube
- B. dynamic application security testing (DAST) by using Veracode
- C. threat modeling by using the Microsoft Threat Modeling Tool
- D. software decomposition by using Microsoft Visual Studio Enterprise



**Answer:** C

**Explanation:**

<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

#### NEW QUESTION 43

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

- A. insider risk management policies
- B. data loss prevention (DLP) policies
- C. sensitivity label policies
- D. retention policies

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

#### NEW QUESTION 47

- (Exam Topic 3)

You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:

- Encrypt cardholder data by using encryption keys managed by the company.
- Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
- B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
- C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
- D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

**Answer:** AC

**Explanation:**

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

#### NEW QUESTION 49

- (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 54

- (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 58

- (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:** BC

**Explanation:**

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

**NEW QUESTION 62**

- (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:** AB

**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 66**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

- A. Microsoft Defender for Cloud Apps
- B. insider risk management
- C. Microsoft Information Protection
- D. Azure Purview

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 67**

- (Exam Topic 3)

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

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

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

Data security:

Access keys stored in Azure Key Vault
Automation Contributor built-in role
Azure Private Link with network service tags
Azure Web Application Firewall rules with network service tags

Network access control:

Access keys stored in Azure Key Vault
Automation Contributor built-in role
Azure Private Link with network service tags
Azure Web Application Firewall rules with network service tags

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Data Security = Access Keys stored in Azure Key Vault

Network access control = Azure Private Link with network service tags

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

**NEW QUESTION 71**

- (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 72**

- (Exam Topic 3)

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

Uploading the code to repositories Building containers

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

Answer Area

Uploading code to repositories:

Azure Boards
Azure Pipelines
GitHub Enterprise
Microsoft Defender for Cloud

Building containers:

Azure Boards
Azure Pipelines
GitHub Enterprise
Microsoft Defender for Cloud

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec> <https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-conta>

**NEW QUESTION 73**

- (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 75

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling the VMAccess extension on all virtual machines.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s> Adaptive Network Hardening:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

#### NEW QUESTION 79

- (Exam Topic 3)

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

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

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 84

- (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 86

- (Exam Topic 3)

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

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

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

Does this meet the goal?

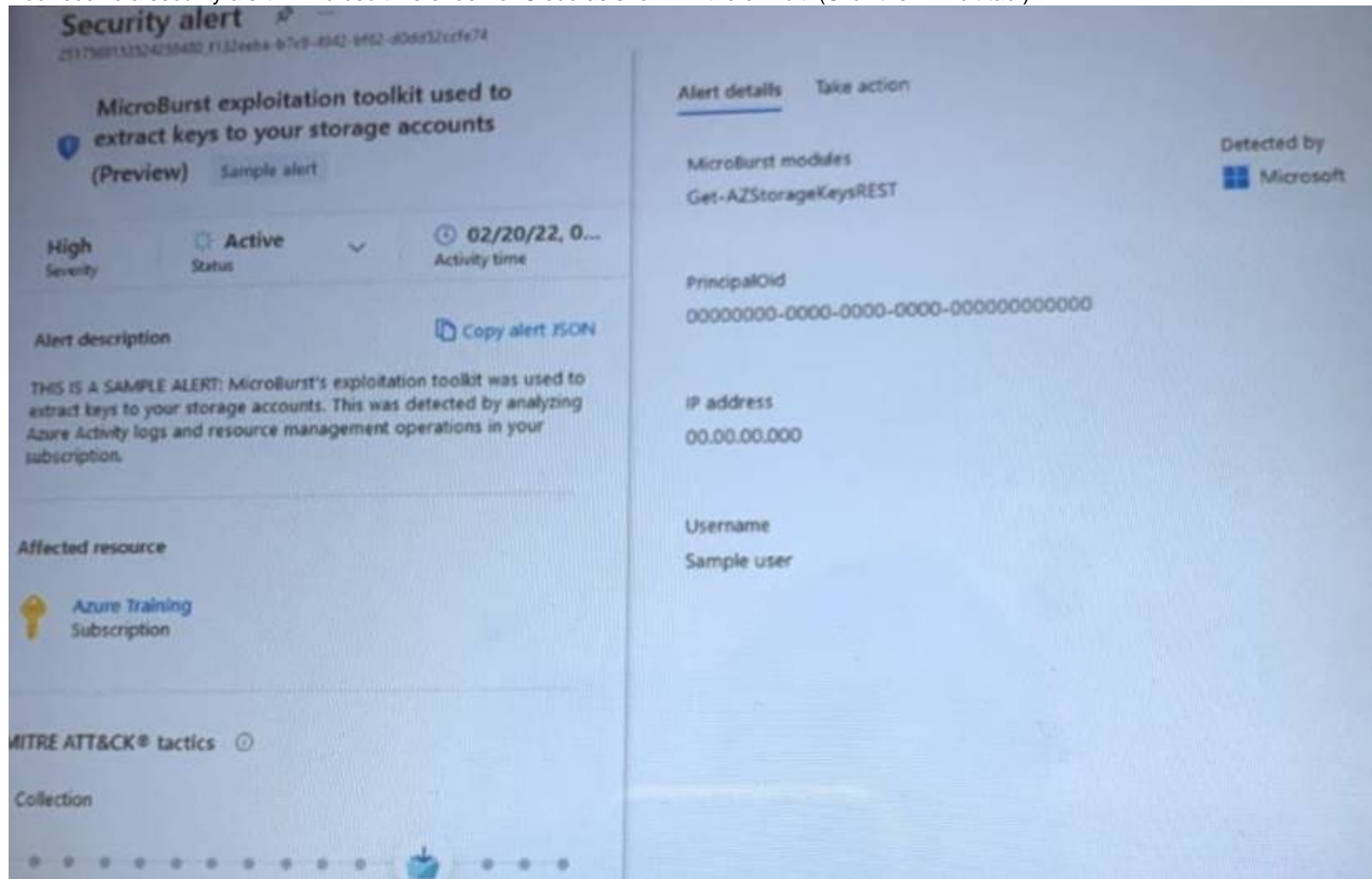
- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 88

- (Exam Topic 3)

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



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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 92

- (Exam Topic 3)

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel. You plan to integrate Microsoft Sentinel with Splunk.

You need to recommend a solution to send security events from Microsoft Sentinel to Splunk. What should you include in the recommendation?

- A. Azure Event Hubs
- B. Azure Data Factor
- C. a Microsoft Sentinel workbook
- D. a Microsoft Sentinel data connector

**Answer:** D

#### Explanation:

<https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-ev>

#### NEW QUESTION 96

- (Exam Topic 3)

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service. You are migrating the on-premises infrastructure to a cloud-only infrastructure.

You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.

Which identity service should you include in the recommendation?

- A. Azure Active Directory Domain Services (Azure AD DS)
- B. Azure Active Directory (Azure AD) B2C
- C. Azure Active Directory (Azure AD)

D. Active Directory Domain Services (AD DS)

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 97

- (Exam Topic 3)

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions. You are evaluating the security posture of the customer.

You discover that the AKS resources are excluded from the secure score recommendations. You need to produce accurate recommendations and update the secure score.

Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

**Answer:** AE

**Explanation:**

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation>

#### NEW QUESTION 99

- (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 103

- (Exam Topic 3)

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

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

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

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

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

- A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
- B. Implement Azure Firewall to restrict host pool outbound access.
- C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
- D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
- E. Deploy a Remote Desktop server to an Azure region located in France.

**Answer:** BCD

**Explanation:**

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

#### NEW QUESTION 106

- (Exam Topic 3)

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

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

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

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

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



point.

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

**Answer:** BC

#### NEW QUESTION 107

- (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 110

- (Exam Topic 3)

Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool. Which type of diagram should you create?

- A. data flow
- B. system flow
- C. process flow
- D. network flow

**Answer:** A

#### Explanation:

<https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram> <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started?source=recommen>

#### NEW QUESTION 113

- (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 118

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### SC-100 Practice Exam Features:

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

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