SC-100$^{Q\&As}$

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

Your company has an Azure App Service plan that is used to deploy containerized web apps.

You are designing a secure DevOps strategy for deploying the web apps to the App Service plan.

You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:

1.

Uploading the code to repositories

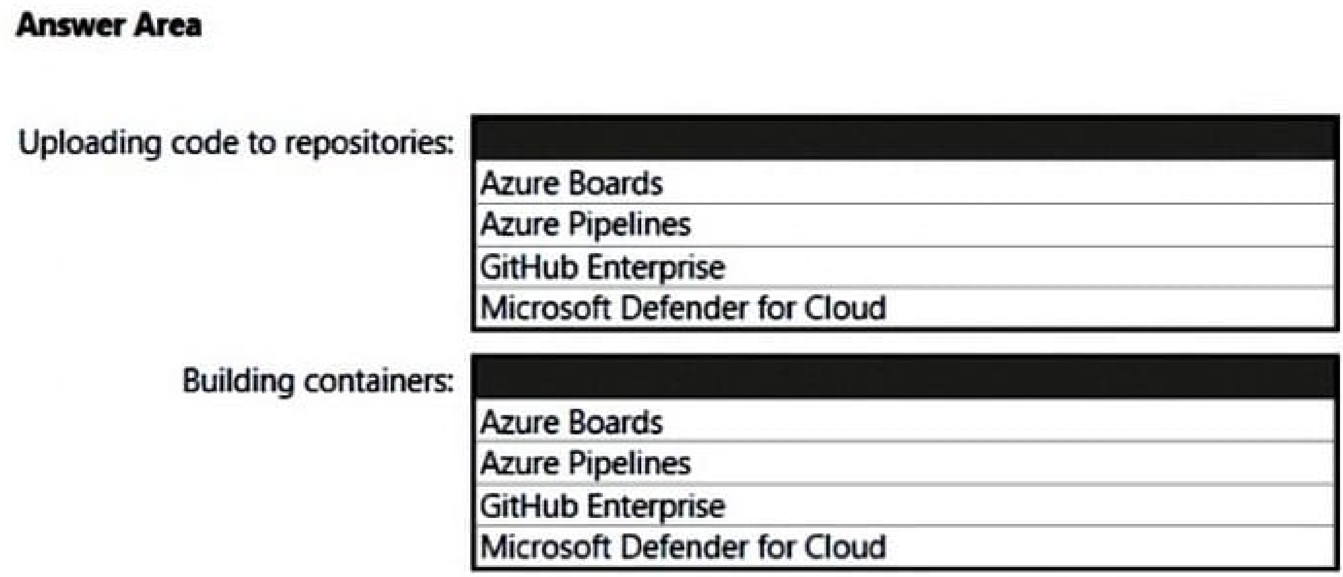
2.

Building containers

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

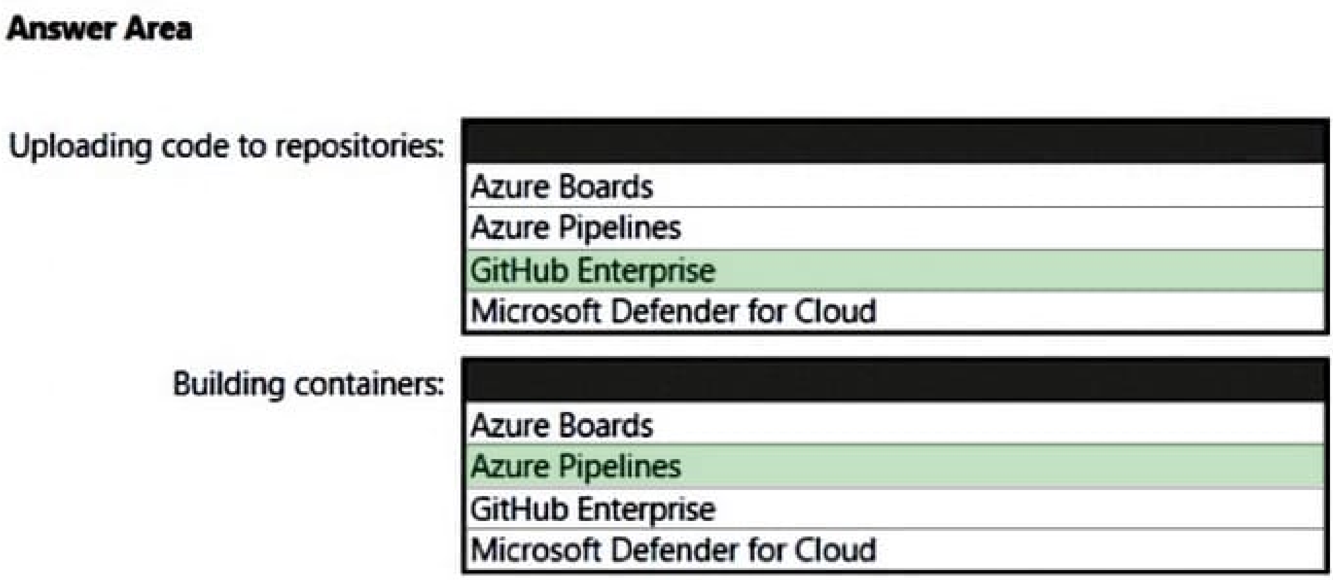
Uploading code to repositories:

- Azure Boards
- Azure Pipelines
- GitHub Enterprise
- Microsoft Defender for Cloud

Building containers:

- Azure Boards
- Azure Pipelines
- GitHub Enterprise
- Microsoft Defender for Cloud

Correct Answer:



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

Box 1: GitHub Enterprise

A GitHub Advanced Security license provides the following additional features:

Code scanning - Search for potential security vulnerabilities and coding errors in your code.

Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also detects secrets when they are pushed to your repository.

Etc.

Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub Enterprise Cloud.

Box 2: Azure Pipelines

Building Containers with Azure DevOps using DevTest Pattern with Azure Pipelines

The pattern enabled as to build container for development, testing and releasing the container for further reuse (production ready).

Azure Pipelines integrates metadata tracing into your container images, including commit hashes and issue numbers from Azure Boards, so that you can inspect your applications with confidence.

Incorrect:

*

Not Azure Boards: Azure Boards provides software development teams with the interactive and customizable tools they need to manage their software projects. It provides a rich set of capabilities including native support for Agile, Scrum,

and Kanban processes, calendar views, configurable dashboards, and integrated reporting.

*

Not Microsoft Defender for Cloud

Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.

You cannot use Microsoft Defender for Cloud to scan code, it scans images.

Reference:

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

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

QUESTION 2

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment.

You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Correct Answer: ACE

RaMP initiatives for Zero Trust

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

Critical security modernization initiatives:

(C) User access and productivity

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

(A) Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

(E) Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

reduce manual effort

Incorrect:

As needed

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

*

(not D) OT and Industrial IoT Discover Protect Monitor

*

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

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

QUESTION 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.

Correct Answer: D

Add a regulatory standard to your dashboard

The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.

Add a standard to your Azure resources

1.

From Defender for Cloud\\'s menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.

2.

From the top of the page, select Manage compliance policies. The Policy Management page appears.

3.

Select the subscription or management group for which you want to manage the regulatory compliance posture.

4.

To add the standards relevant to your organization, expand the Industry and regulatory standards section and select Add more standards.

5.

From the Add regulatory compliance standards page, you can search for any of the available standards:

6.

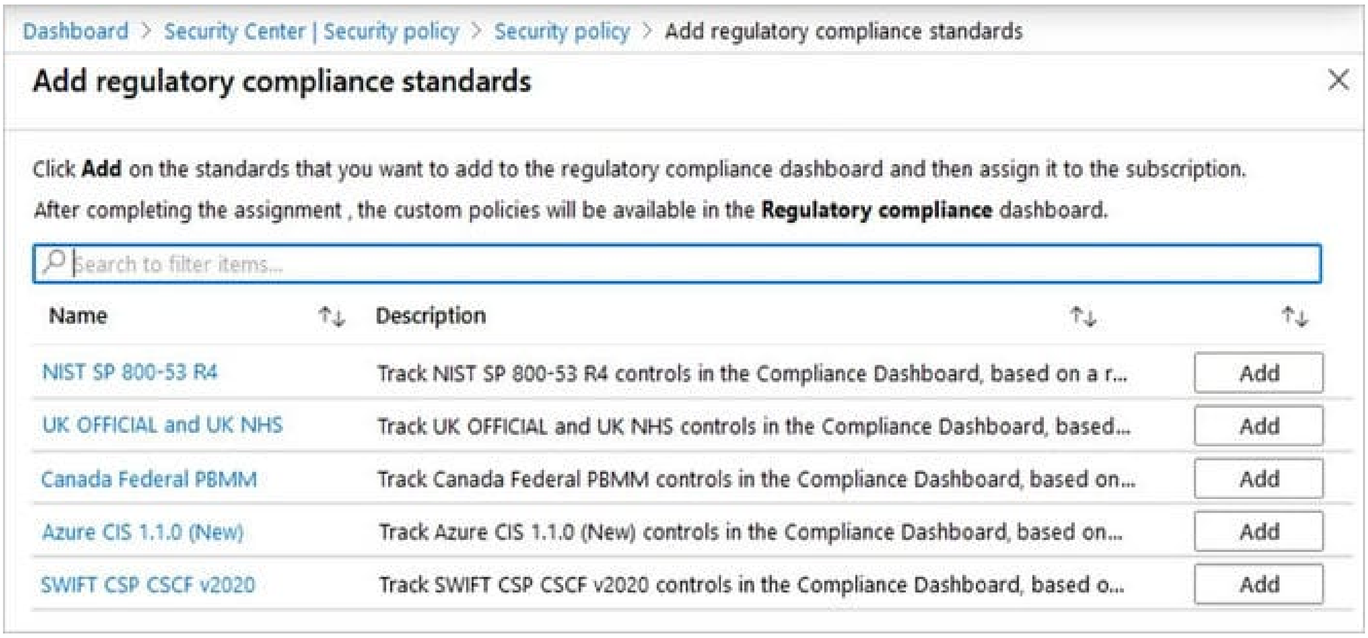
Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.

7.

From Defender for Cloud\\'s menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.

Your new standard appears in your list of Industry and regulatory standards.

Note: Customize the set of standards in your regulatory compliance dashboard.



Dashboard > Security Center | Security policy > Security policy > Add regulatory compliance standards

Add regulatory compliance standards

Click **Add** on the standards that you want to add to the regulatory compliance dashboard and then assign it to the subscription.
After completing the assignment , the custom policies will be available in the **Regulatory compliance** dashboard.

Search to filter items...

Name ↑↓	Description ↑↓	↑↓
NIST SP 800-53 R4	Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a r...	Add
UK OFFICIAL and UK NHS	Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based...	Add
Canada Federal PBMM	Track Canada Federal PBMM controls in the Compliance Dashboard, based on...	Add
Azure CIS 1.1.0 (New)	Track Azure CIS 1.1.0 (New) controls in the Compliance Dashboard, based on...	Add
SWIFT CSP CSCF v2020	Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based o...	Add

Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you\\'re meeting specific compliance requirements. Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

QUESTION 4

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 Defender for Endpoint

B. Microsoft Endpoint Manager

C. Microsoft Information Protection

D. Microsoft Sentinel

Correct Answer: B

Microsoft Endpoint Manager includes Microsoft Intune.

Device compliance policies are a key feature when using Intune to protect your organization\\'s resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version.

Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint Manager includes the services and tools you use to manage and monitor mobile

devices, desktop computers, virtual machines, embedded devices, and servers.

Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. These services are part of the Microsoft 365 stack to

help secure access, protect data, respond to risk, and manage risk.

Note: Microsoft Defender for Endpoint Plan 2 protects your Windows and Linux machines whether they\\'re hosted in Azure, hybrid clouds (on-premises), or multicloud.

Microsoft Defender for Endpoint on iOS offers protection against phishing and unsafe network connections from websites, emails, and apps.

Microsoft Defender for Endpoint on Android supports installation on both modes of enrolled devices - the legacy Device Administrator and Android Enterprise modes. Currently, Personally-owned devices with work profile and Corporate-

owned fully managed user device enrollments are supported in Android Enterprise.

Reference: https://docs.microsoft.com/en-us/mem/endpoint-manager-overview https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint

QUESTION 5

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. Azure AD Conditional Access

B. Azure Data Catalog

C. Microsoft Purview Information Protection

D. Azure AD Application Proxy

E. Microsoft Defender for Cloud Apps

Correct Answer: AE

Explanation:

Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies.

Create a block download policy for unmanaged devices

Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of a session using its device as a condition, create both a conditional access policy AND a session policy.

Incorrect:

Not B: Azure Data Catalog is an enterprise-wide metadata catalog that makes data asset discovery straightforward. It\\'s a fully-managed service that lets you — from analyst to data scientist to data developer — register, enrich, discover,

understand, and consume data sources.

Not C: Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.

Reference:

https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad