SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 a workflow automation feature of Microsoft Defender for Cloud.

What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Event Hubs

C. Azure Functions apps

D. Azure Logic Apps

Correct Answer: D

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.

Incorrect:

Not C: Using Azure Functions apps would require more effort.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

QUESTION 2

HOTSPOT

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII).

The company plans to use Microsoft Information Protection for the PII data store in Azure.

You need to recommend a solution to discover PII data at risk in the Azure resources.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Correct Answer:

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- **Azure Purview**
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- **Microsoft Defender for Cloud**
- Microsoft Defender for Cloud Apps

Box 1: Azure Purview

Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data. Microsoft Purview allows you to:

Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

Enable data curators to manage and secure your data estate.

Empower data consumers to find valuable, trustworthy data.

Box 2: Microsoft Defender for Cloud

Microsoft Purview provides rich insights into the sensitivity of your data. This makes it valuable to security teams using Microsoft Defender for Cloud to manage the organization\\'s security posture and protect against threats to their workloads.

Data resources remain a popular target for malicious actors, making it crucial for security teams to identify, prioritize, and secure sensitive data resources across their cloud environments. The integration with Microsoft Purview expands

visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.

References: https://docs.microsoft.com/en-us/azure/purview/overview

https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

QUESTION 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.

Correct Answer: ACE

QUESTION 4

You have an on-premises network and a Microsoft 365 subscription.

You are designing a Zero Trust security strategy.

Which two security controls should you include as part of the Zero Trust solution? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Always allow connections from the on-premises network.

B. Disable passwordless sign-in for sensitive accounts.

C. Block sign-in attempts from unknown locations.

D. Block sign-in attempts from noncompliant devices.

Correct Answer: CD

QUESTION 5

HOTSPOT

You use Azure Policy with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows.

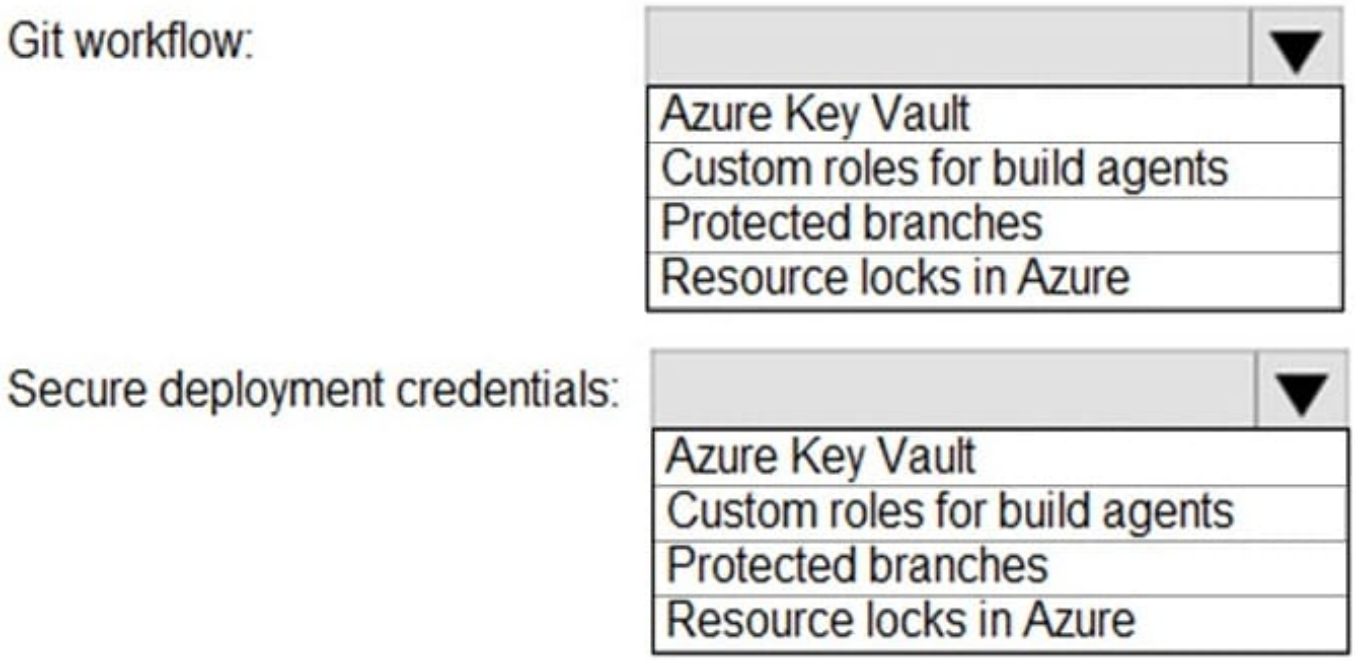
You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.

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

NOTE: Each correct selection is worth one point.

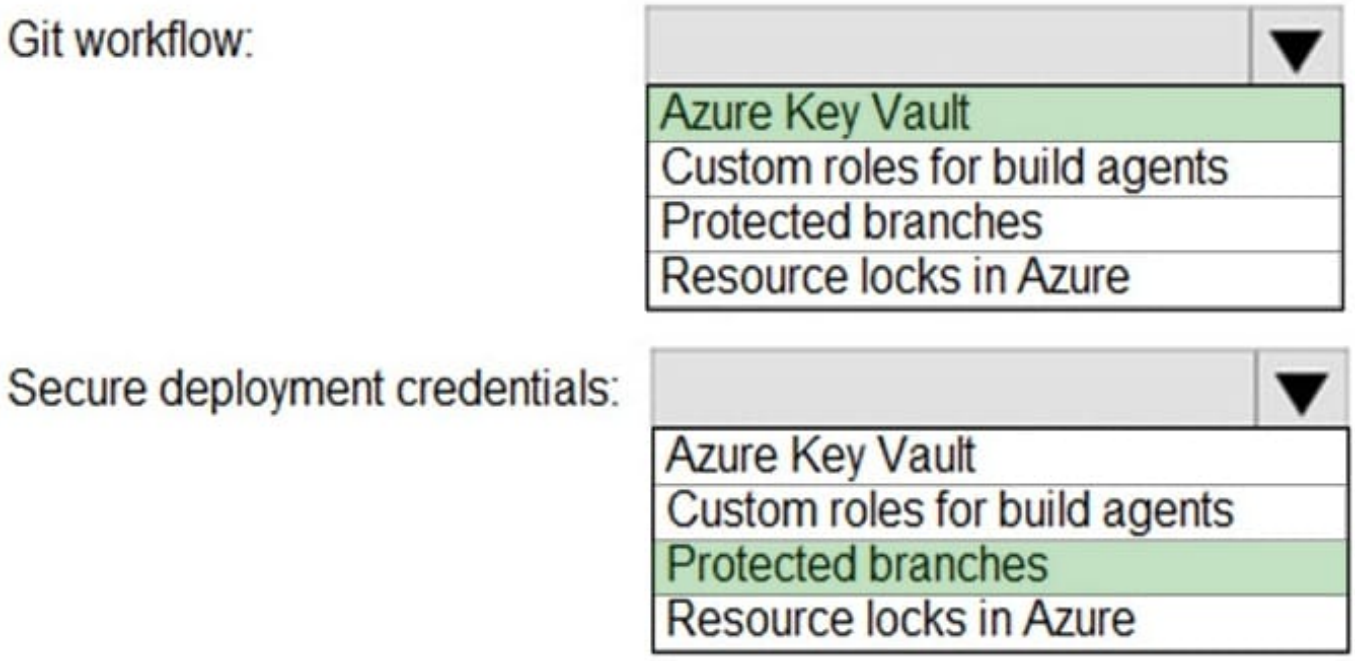
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Protected branches

Git workflow

The pull request workflow is designed to introduce healthy friction, which is why it should only be applied to secure specific Git branches. Especially the branches that will trigger automated workflows that can deploy, configure, or in any other

way affect your cloud resources. These branches are called protected branches.

Restrict access to protected branches

The pull request workflow is used together with restricted access controls. The pull request workflow can\\'t be enforced however, unless the server is configured to reject direct changes to protected branches.

A developer can\\'t push directly to the production branch, but instead must create a pull request that targets the protected branch. Each SCM vendor has a different flavor for achieving restricted access to protected branches. For example, with

GitHub this feature is only available for organizations using GitHub team or GitHub Enterprise cloud.

Box 2: Azure Key Vault

Secure your deployment credentials

Pipelines and code repositories should not include hard-coded credentials and secrets. Credentials and secrets should be stored elsewhere and use CI vendor features for security. Because pipelines run as headless agents, they should

never use an individual\\'s password.

Azure Key Vault

If your CI platform supports it, consider storing credentials in a dedicated secret store, for example Azure Key Vault. Credentials are fetched at runtime by the build agent and your attack surface is reduced.

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops