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.pass2lead.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

Your company has an on-premises network and an Azure subscription.

The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.

You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.

You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.

What should you include in the recommendation?

A. a private endpoint

B. hybrid connections

C. virtual network NAT gateway integration

D. virtual network integration

Correct Answer: B

Hybrid Connections can connect Azure App Service Web Apps to on-premises resources that use a static TCP port. Supported resources include Microsoft SQL Server, MySQL, HTTP Web APIs, Mobile Services, and most custom Web

Services.

Note: You can use an Azure App Service Hybrid Connections. To do this, you need to add and create Hybrid Connections in your app. You will download and install an agent (the Hybrid Connection Manager) in the database server or another

server which is in the same network as the on-premise database.

You configure a logical connection on your app service or web app.

A small agent, the Hybrid Connection Manager, is downloaded and installed on a Windows Server (2012 or later) running in the remote network (on-premises or anywhere) that you need to communicate with.

You log into your Azure subscription in the Hybrid Connection manager and select the logical connection in your app service.

The Hybrid Connection Manager will initiate a secure tunnel out (TCP 80/443) to your app service in Azure.

Your app service can now communicate with TCP-based services, on Windows or Linux, in the remote network via the Hybrid Connection Manager.

You could get more details on how to Connect Azure Web Apps To On-Premises.

Incorrect:

Not A: NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway

specifies which static IP addresses virtual machines use when creating outbound flows.

However, we need an inbound connection.

Not C: You can Azure web app service VNet integration with Azure VPN gateway to securely access the resource in an Azure VNet or on-premise network.

Note: Virtual network integration gives your app access to resources in your virtual network, but it doesn\\'t grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a

private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network. The virtual network integration feature behaves differently when it\\'s used

with virtual networks in the same region and with virtual networks in other regions. The virtual network integration feature has two variations:

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you\\'re integrating with.

Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

Reference: https://github.com/uglide/azure-content/blob/master/articles/app-service-web/web-sites-hybrid-connection-connect-on-premises-sql-server.md

https://docs.microsoft.com/en-us/answers/questions/701793/connecting-to-azure-app-to-onprem-datbase.html

---

QUESTION 2

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.

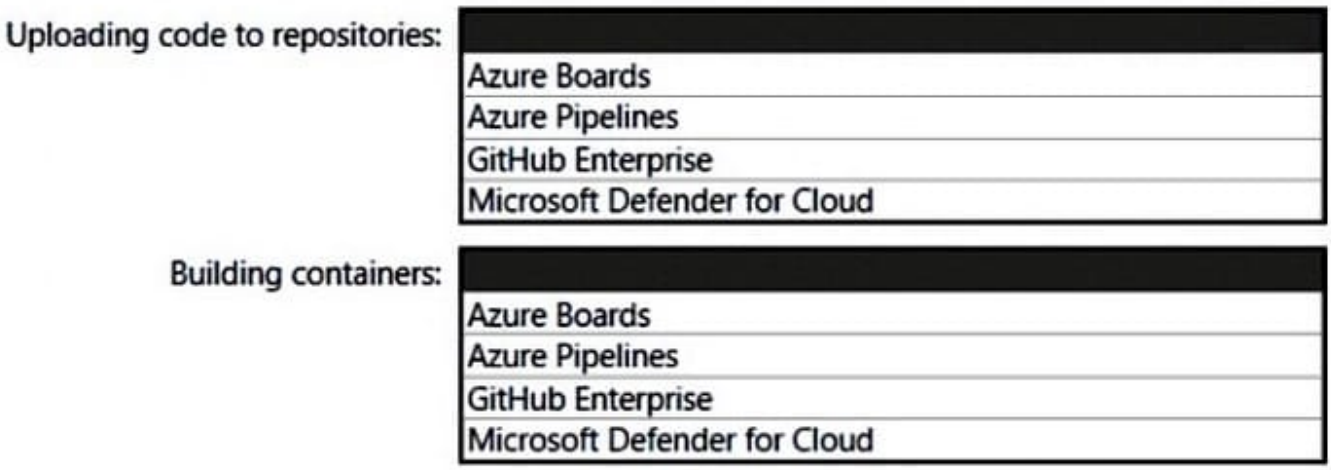
Building containers

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.

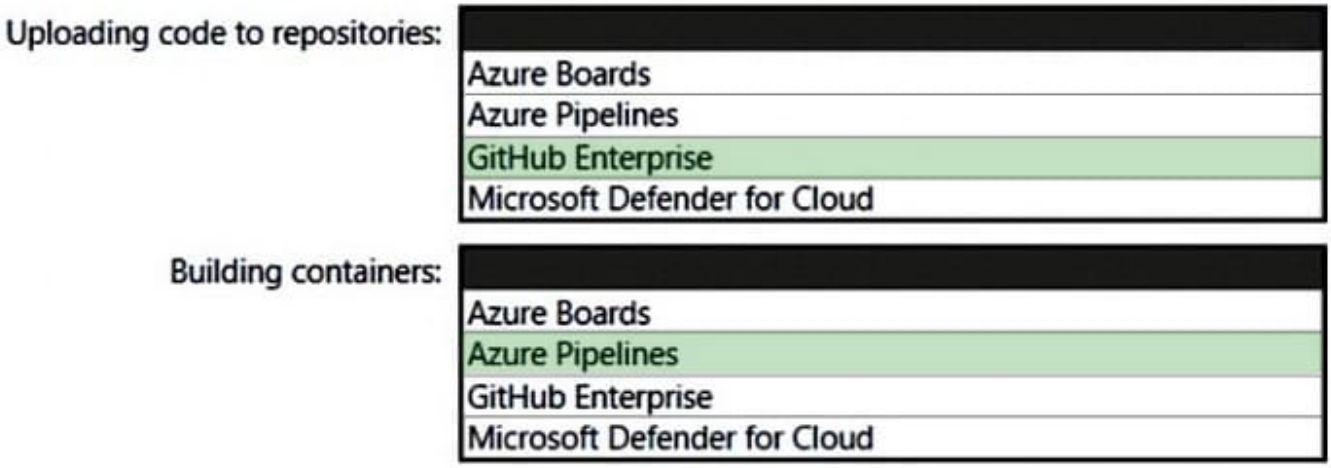
Hot Area:

Answer Area



Correct Answer:

Answer Area



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 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 AD Conditional Access App Control policies

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app protection policies in Microsoft Endpoint Manager

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: D

Explanation:

Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

Note: Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

Incorrect:

Not C: App protection policies (APP) are rules that ensure an organization\\'s data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of

actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization\\'s data within an application. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM.

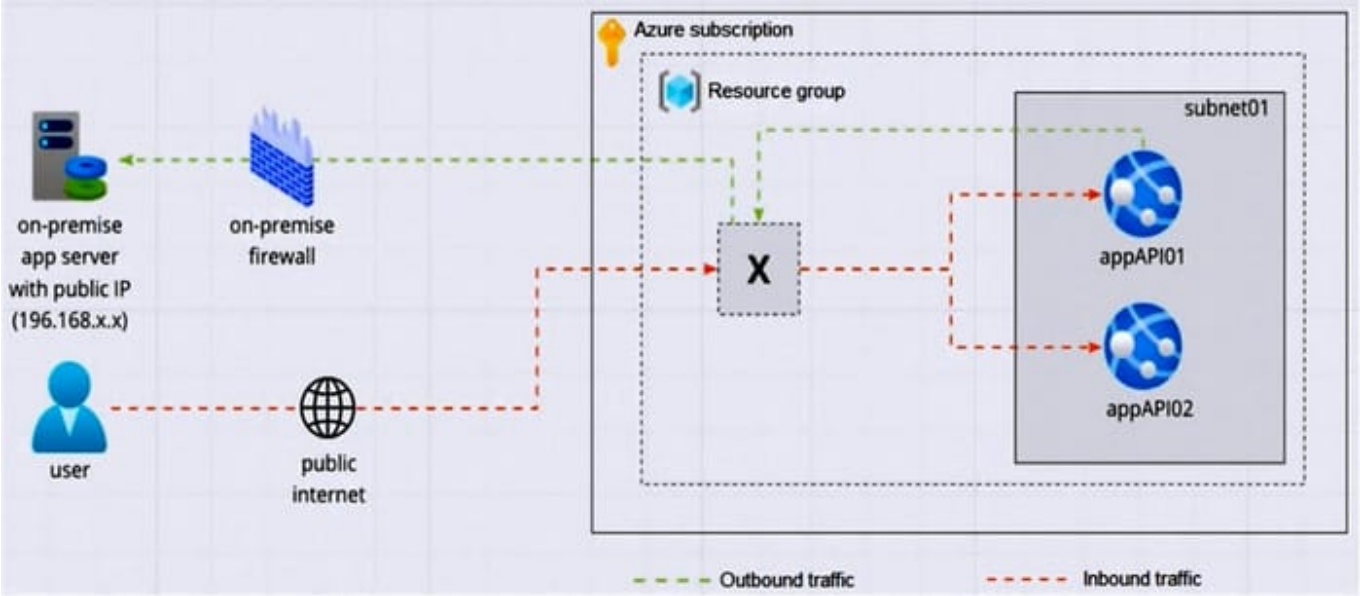
Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy

QUESTION 4

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Firewall with policy rule sets

C. Azure Front Door with Azure Web Application Firewall (WAF)

D. Azure Application Gateway v2 with user-defined routes (UDRs)

Correct Answer: B

https://learn.microsoft.com/en-us/azure/app-service/environment/firewall-integration

QUESTION 5

DRAG DROP

You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

1.

User accounts that were potentially compromised

2.

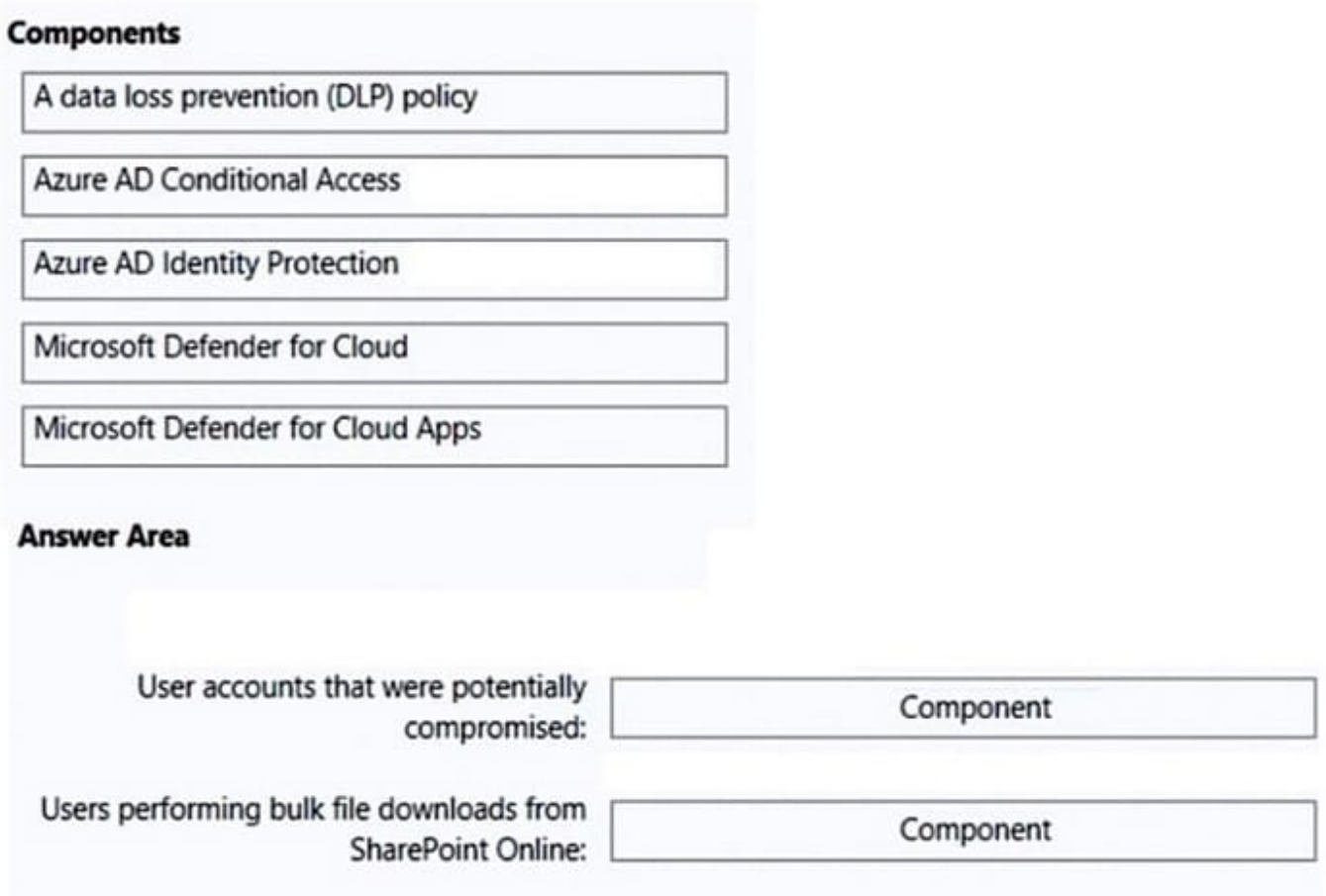
Users performing bulk file downloads from Microsoft SharePoint Online

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

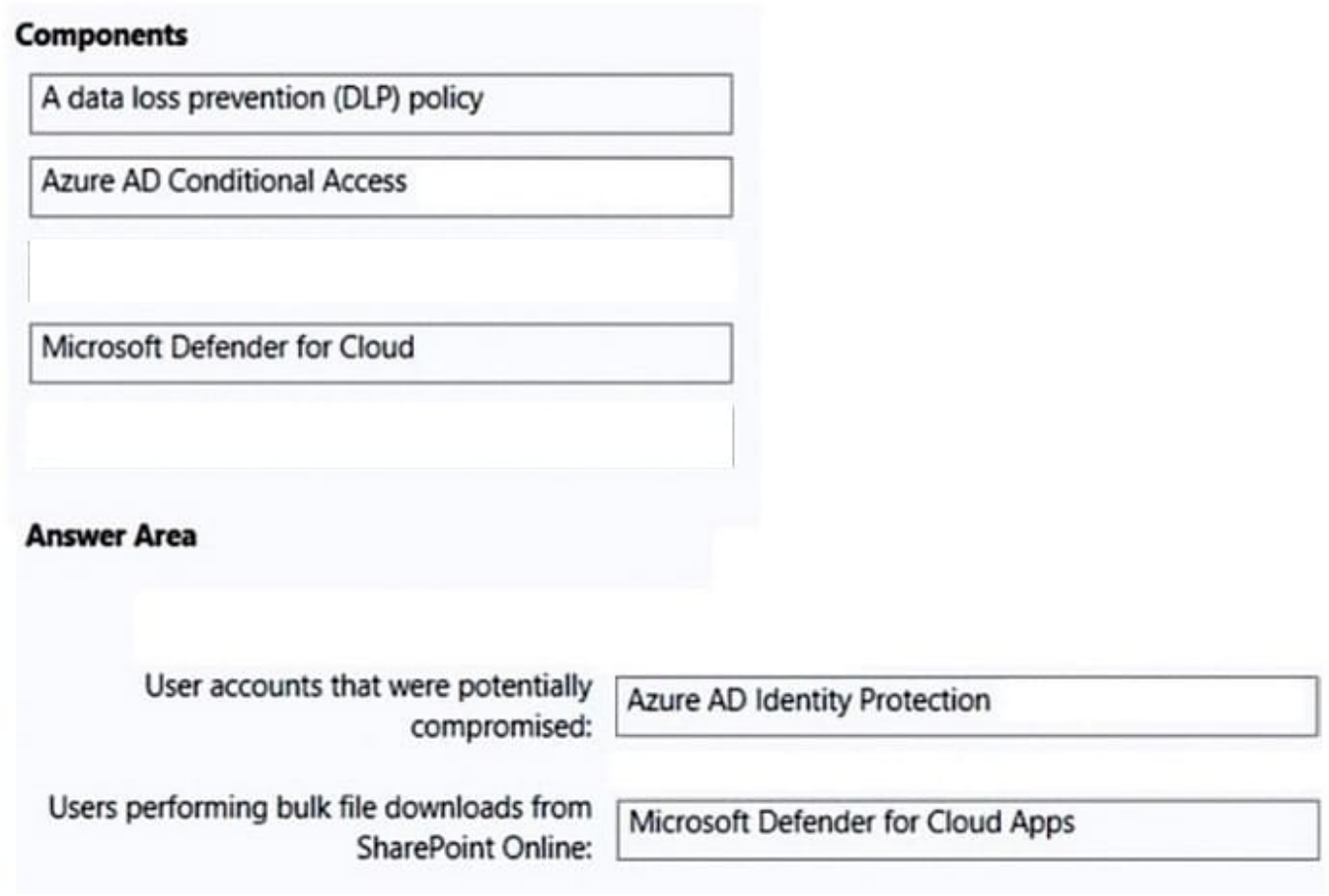
between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky

Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

Premium sign-in risk detections include:

*

Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.

*

Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user\\'s inbox. This detection may indicate that the user\\'s account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.

*

Etc.

Incorrect:

Not: Microsoft 365 Defender for Cloud

Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365 Defender portal from Incidents and alerts > incident > Users.

Box 2: Microsoft 365 Defender for App

Defender for Cloud apps detect mass download (data exfiltration) policy

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

Reference: 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-exfiltration
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users