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.geekcert.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

HOTSPOT

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.

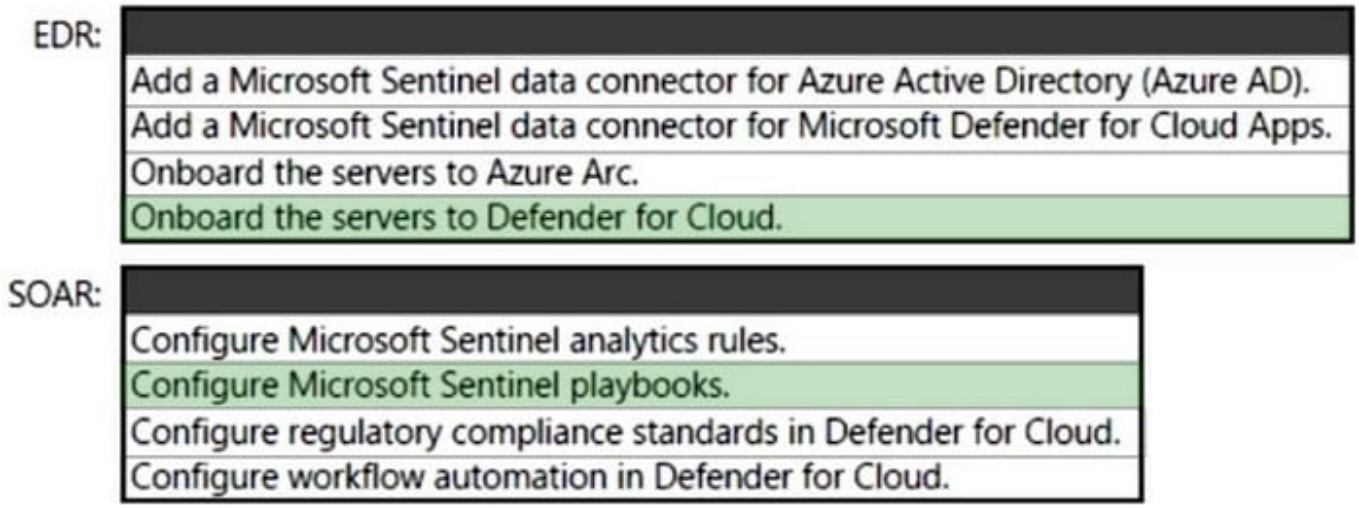
Hot Area:

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.

Correct Answer:

Answer Area



Box 1: Onboard the servers to Defender for Cloud.

Extended detection and response (XDR) is a new approach defined by industry analysts that are designed to deliver intelligent, automated, and integrated security across domains to help defenders connect seemingly disparate alerts and get

ahead of attackers.

As part of this announcement, we are unifying all XDR technologies under the Microsoft Defender brand. The new Microsoft Defender is the most comprehensive XDR in the market today and prevents, detects, and responds to threats across

identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

Box 2: Configure Microsoft Sentinel playbooks.

As a SOAR platform, its primary purposes are to automate any recurring and predictable enrichment, response and remediation tasks that are the responsibility of Security Operations Centers (SOC/SecOps). Leveraging SOAR frees up time

and resources for more in-depth investigation of and hunting for advanced threats. Automation takes a few different forms in Microsoft Sentinel, from automation rules that centrally manage the automation of incident handling and response to

playbooks that run predetermined sequences of actions to provide robust and flexible advanced automation to your threat response tasks.

Reference: https://www.microsoft.com/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-automation-ninja/ba-p/3563377

QUESTION 2

HOTSPOT

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to evaluate the existing environment to increase the overall security posture for the following components:

1.

Windows 11 devices managed by Microsoft Intune

2.

Azure Storage accounts

3.

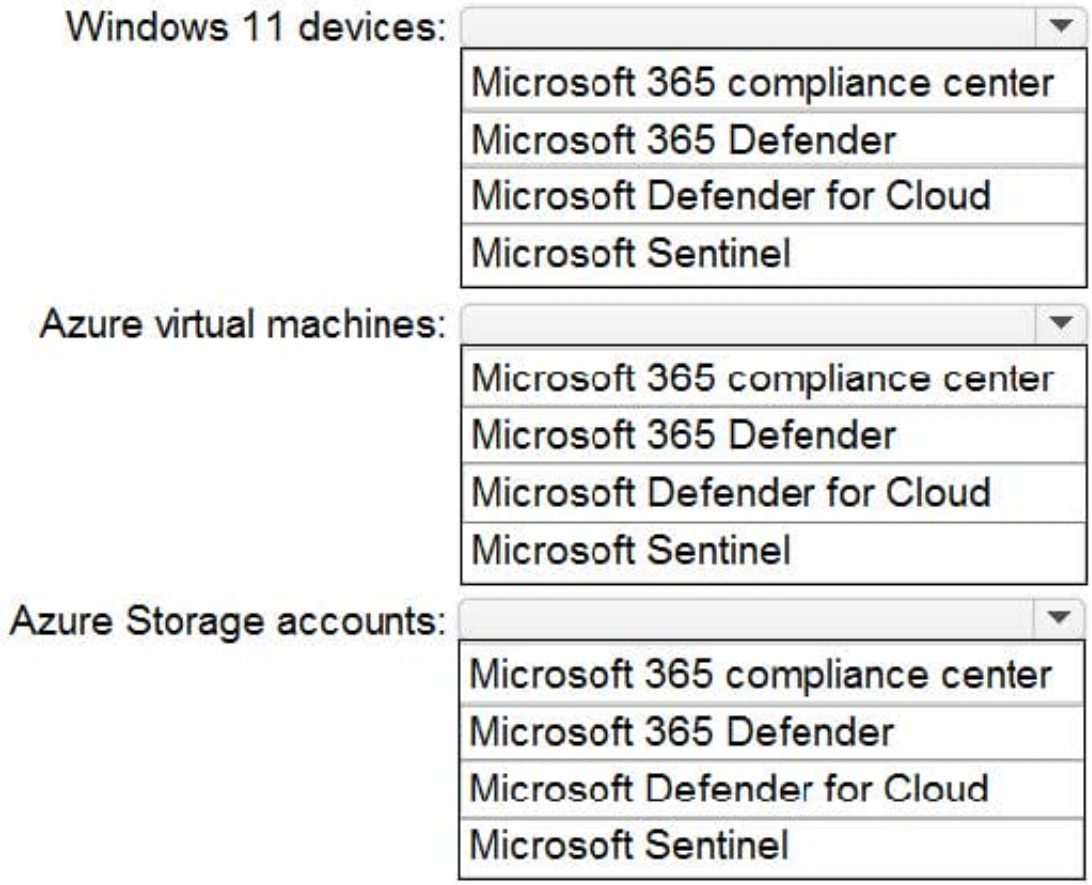
Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

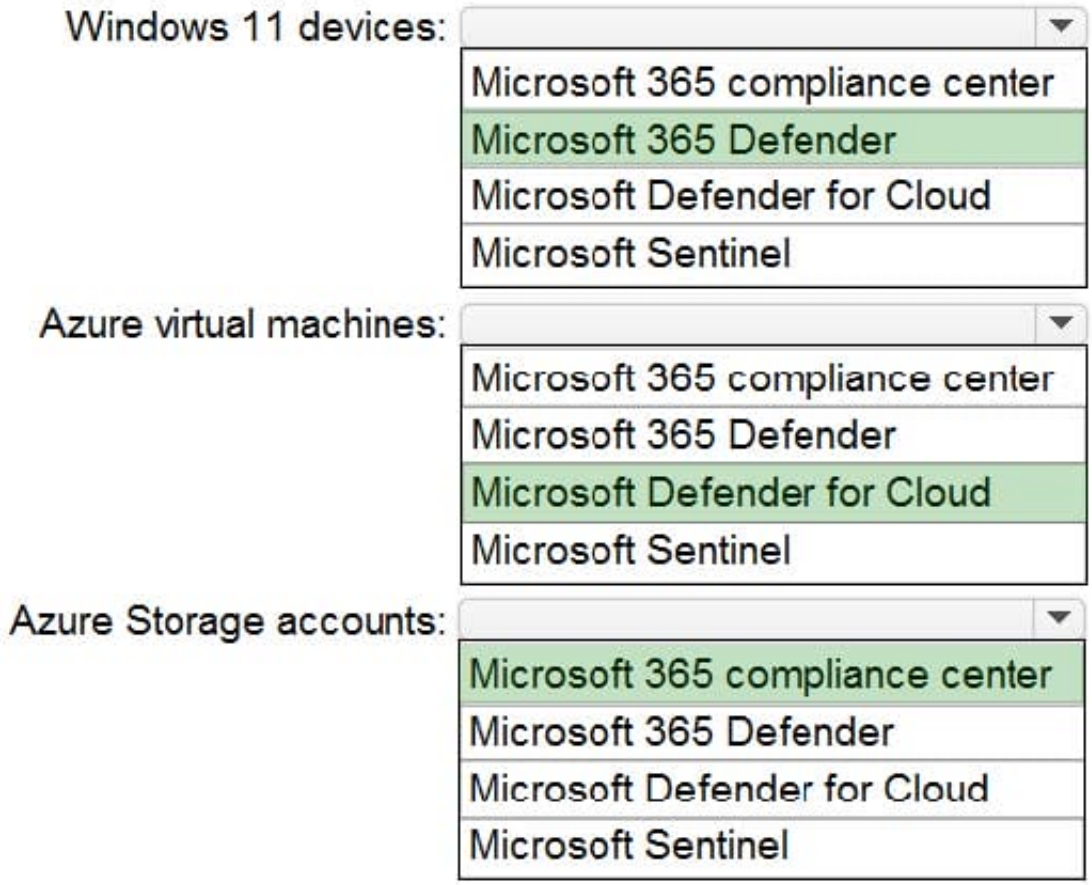
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Microsoft 365 Defender

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Microsoft Defender for Endpoint works with devices that run:

Android

iOS/iPadOS

Windows 10

Windows 11

Box 2: Microsoft Defender for Cloud

Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed

Instance and Azure Virtual Machines.

Box 3: Microsoft 365 Compliance Center

Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.

Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.

Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.

Reference: https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint

https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

QUESTION 3

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You need to enforce ISO 27001:2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically.

What should you use?

A. Azure Policy

B. Azure Blueprints

C. the regulatory compliance dashboard in Defender for Cloud

D. Azure role-based access control (Azure RBAC)

Correct Answer: A

Control mapping of the ISO 27001 Shared Services blueprint sample

The following mappings are to the ISO 27001:2013 controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an Azure Policy initiative.

Open Policy in the Azure portal and select the Definitions page. Then, find and select the [Preview] Audit ISO 27001:2013 controls and deploy specific VM Extensions to support audit requirements built-in policy initiative.

Note: Security Center can now auto provision the Azure Policy\\'s Guest Configuration extension (in preview)

Azure Policy can audit settings inside a machine, both for machines running in Azure and Arc connected machines. The validation is performed by the Guest Configuration extension and client.

With this update, you can now set Security Center to automatically provision this extension to all supported machines.

Enforcing a secure configuration, based on a specific recommendation, is offered in two modes:

Using the Deny effect of Azure Policy, you can stop unhealthy resources from being created

Using the Enforce option, you can take advantage of Azure Policy\\'s DeployIfNotExist effect and automatically remediate non-compliant resources upon creation Reference: https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive https://docs.microsoft.com/en-us/azure/defender-for-cloud/prevent-misconfigurations

QUESTION 4

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. Enable Defender plans.

B. Configure auto provisioning.

C. Add a workflow automation.

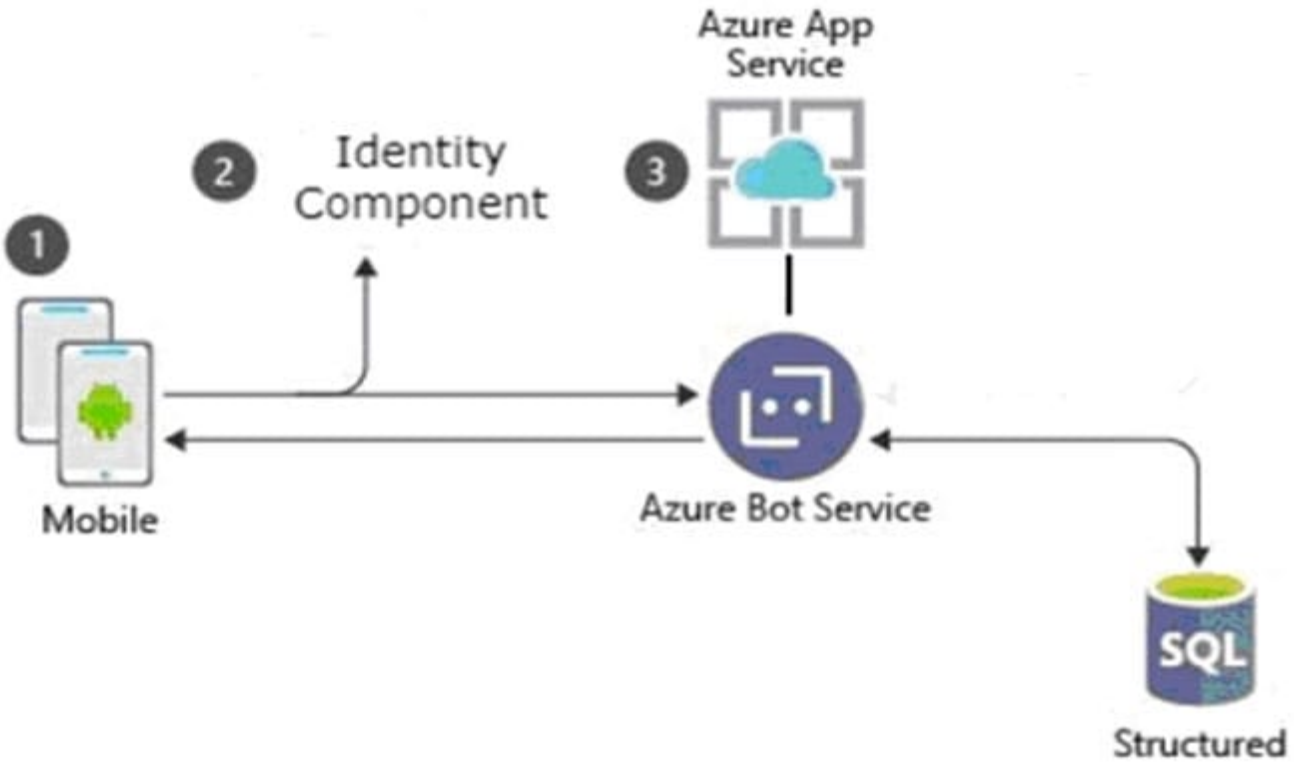
D. Assign regulatory compliance policies.

E. Review the inventory.

Correct Answer: AB

QUESTION 5

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

1.

Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.

2.

Be managed separately from the identity store of the customer.

3.

Support fully customizable branding for each app. Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2B

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD) B2C

D. Azure AD Connect

Correct Answer: C

Azure Active Directory B2C (Azure AD B2C), an identity store, is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page

(SPA), and other applications.

You can set up sign-up and sign-in with a Facebook/Google account using Azure Active Directory B2C.

Branding

Branding and customizing the user interface that Azure Active Directory B2C (Azure AD B2C) displays to your customers helps provide a seamless user experience in your application. These experiences include signing up, signing in, profile

editing, and password resetting. This article introduces the methods of user interface (UI) customization.

Incorrect:

Not D: Azure AD Connect is a tool for connecting on-premises identity infrastructure to Microsoft Azure AD.

Reference: https://docs.microsoft.com/en-us/azure/active-directory-b2c/

https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow

https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow