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

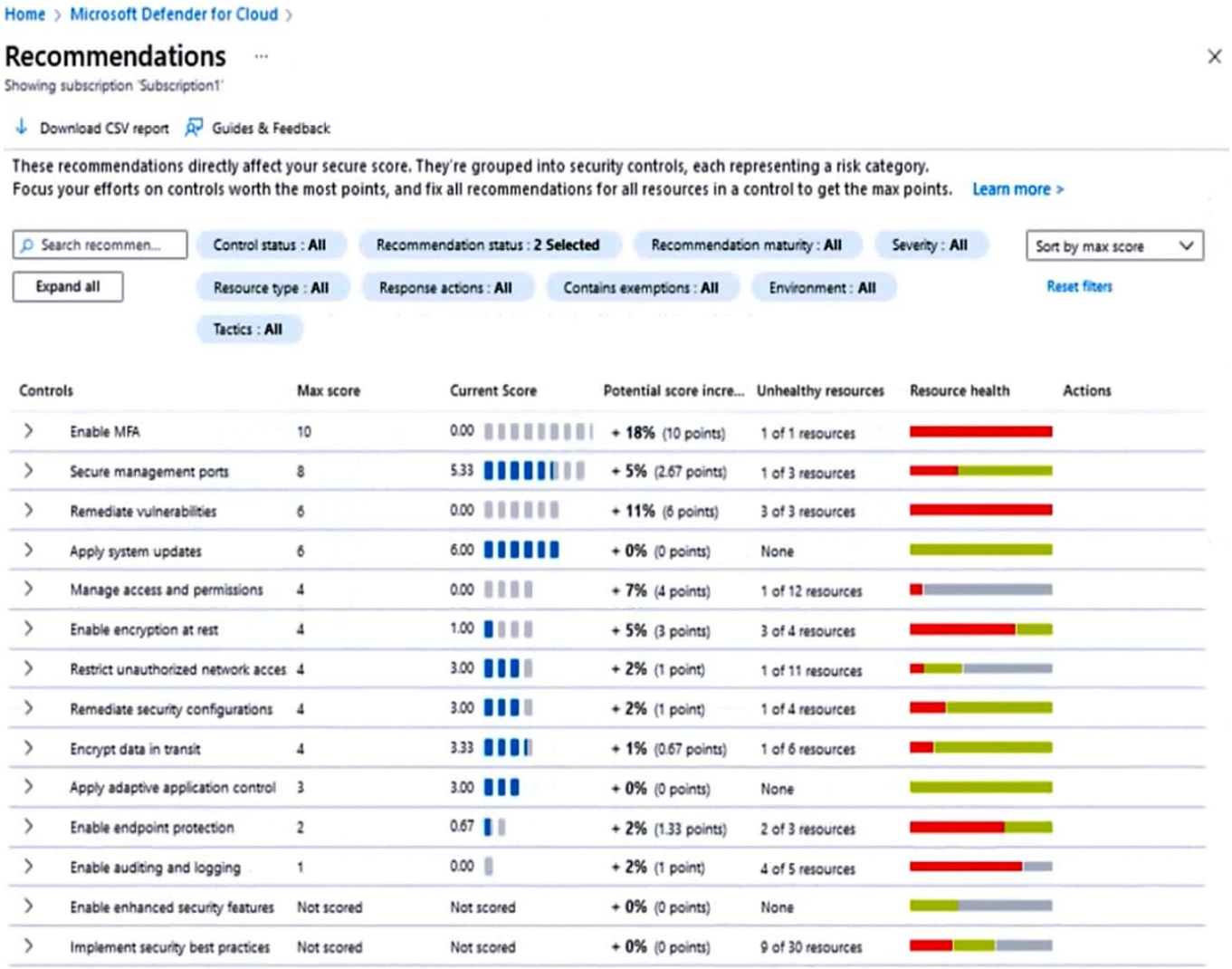
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

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



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Azure AD Conditional Access policies
Azure Web Application Firewall (WAF)
network security groups (NSGs)

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

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

Correct Answer:

Answer Area

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

Azure AD Conditional Access policies
Azure Web Application Firewall (WAF)
network security groups (NSGs)

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

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

Box 1: Azure Web Application Firewall (WAF)

Restrict unauthorized network access control: 1 resource out of 11 needs to be addresses.

Restrict unauthorized network access - Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.

Use these recommendations to manage Defender for Cloud\\'s adaptive network hardening settings, ensure you configured Azure Private Link for all relevant PaaS services, enable Azure Firewall on your virtual networks, and more.

Note: Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway.

Azure WAF protects inbound traffic to the web workloads, and the Azure Firewall inspects inbound traffic for the other applications. The Azure Firewall will cover outbound flows from both workload types.

Incorrect:

Not network security groups (NSGs).

Box 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization\\'s endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn\\'t found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

Incorrect:

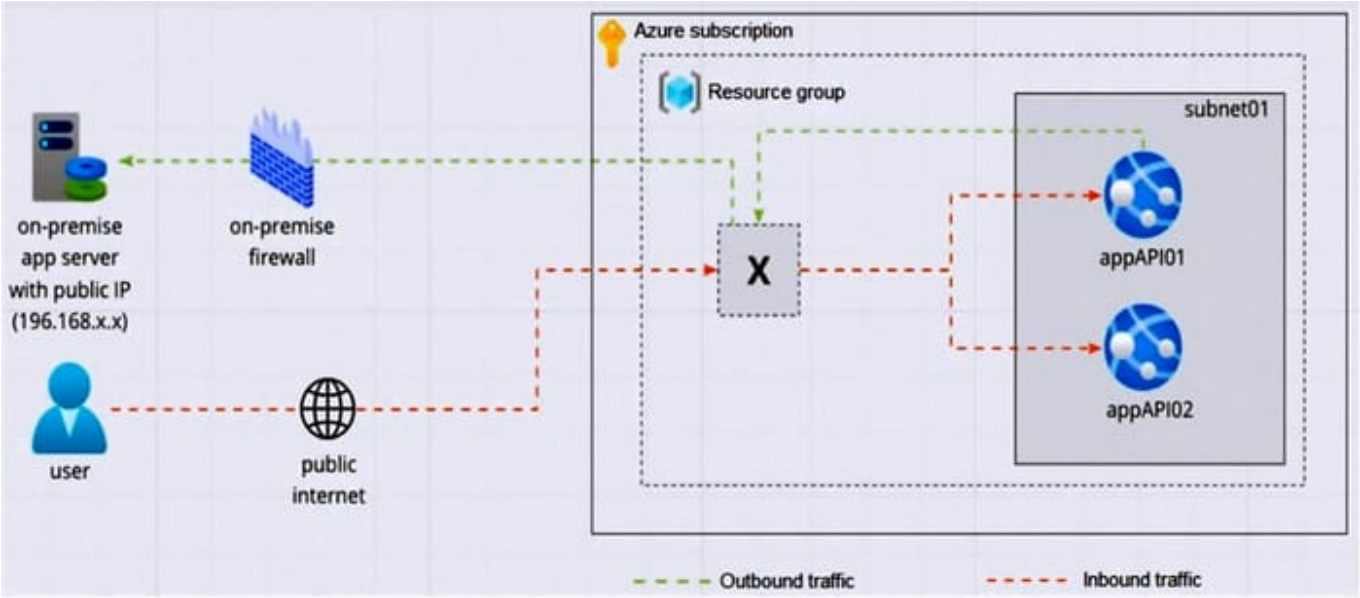
Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they\\'re performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity. Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 2

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 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. Azure AD Privileged Identity Management (PIM)

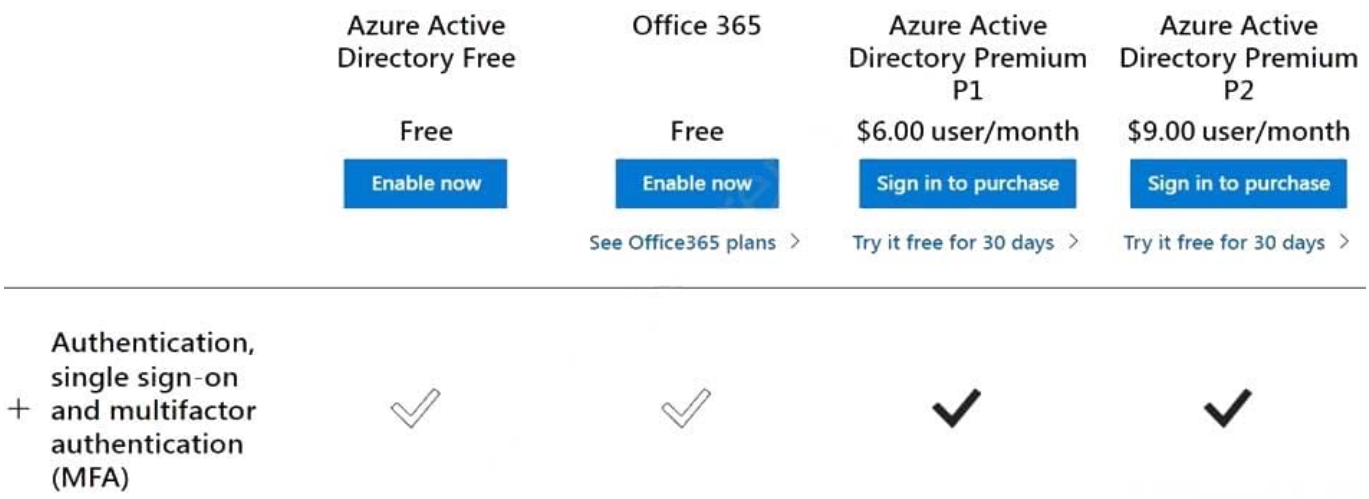
B. role-based authorization

C. resource-based authorization

D. Azure AD Multi-Factor Authentication

Correct Answer: D

Multifactor authentication (MFA), an important component of the Zero Trust Model, is missing in Azure AD Free edition.



QUESTION 4

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

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.

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 5

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Security Assertion Markup Language (SAML)

B. NTLMv2

C. certificate-based authentication

D. Kerberos

Correct Answer: AD

A: SAML

Litware identifies the following application security requirements:

Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

You can provide single sign-on (SSO) to on-premises applications that are secured with SAML authentication and provide remote access to these applications through Application Proxy. With SAML single sign-on, Azure Active Directory (Azure AD) authenticates to the application by using the user\\'s Azure AD account.

D: You can provide single sign-on for on-premises applications published through Application Proxy that are secured

with integrated Windows authentication. These applications require a Kerberos ticket for access. Application Proxy uses Kerberos Constrained Delegation (KCD) to support these applications.

Incorrect:

Not C: Certificate. This is not a custom domain scenario!

If you\\'re using a custom domain, you also need to upload the TLS/SSL certificate for your application.

To configure an on-premises app to use a custom domain, you need a verified Azure Active Directory custom domain, a PFX certificate for the custom domain, and an on-premises app to configure.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain