Free Questions for SC-100 by ebraindumps

Shared by Becker on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

You have a Microsoft 365 tenant.

You need to recommend a Microsoft 365 Defender solution to enhance security for the tenant. The solution must meet the following requirements:

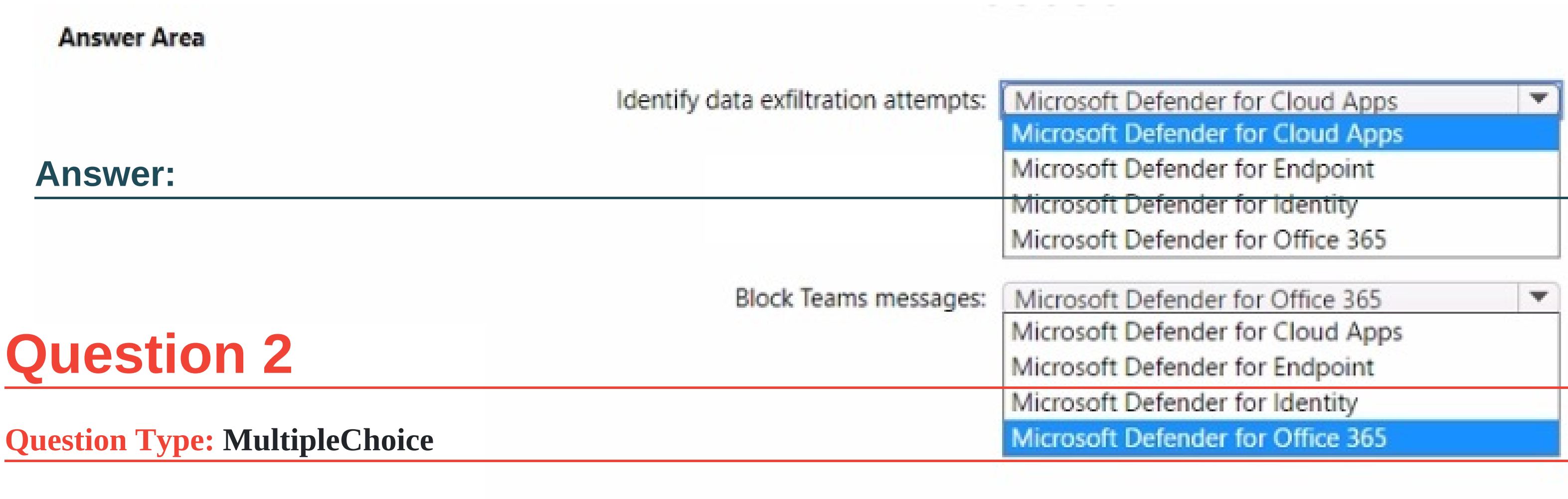
* Identify users that are downloading an unusually high number of files from Microsoft SharePoint Online sites and are possibly involved in a data exfiltration attempt.

* Block Microsoft Teams messages that contain potentially malicious content by using zero-hour auto purge (ZAP).

What should you recommend for each requirement? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer:



Answer Area

Identify data exfiltration attempts: Microsoft Defender for Cloud Apps

- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365

Block Teams messages: Microsoft Defender for Office 365

- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365

Question 2

Question Type: **MultipleChoice**

You have a Microsoft 365 tenant that contains 5,000 users and 5,000 Windows 11 devices. All users are assigned Microsoft 365 5 licenses and the Microsoft Defender Vulnerability Management add-on. The Windows 11 devices are managed by using Microsoft Intune and Microsoft Defender for Endpoint. The Windows 11 devices are configured during deployment to comply with Center for Internet Security (CIS) benchmarks for Windows 11.

You need to recommend a compliance solution for the Windows 11 devices. The solution must identify devices that were modified and no longer comply with the CIS benchmarks.

What should you include in the recommendation?

Options:

A- Authenticated scan for Windows in Microsoft Defender Vulnerability Management

B- Microsoft Secure Score for Devices in Defender for Endpoint

C- attack surface reduction (ASR) rules in Defender for Endpoint

D- security baselines assessments in Microsoft Defender Vulnerability Management

Answer:

D

Question 3

Question Type: **MultipleChoice**

Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

What should you recommend?

Options:

A- Compliance Manager in Microsoft Purview

B- Microsoft Defender for Cloud

C- Microsoft Sentinel

D- Microsoft Defender for Cloud Apps

Answer:

D

Question 4

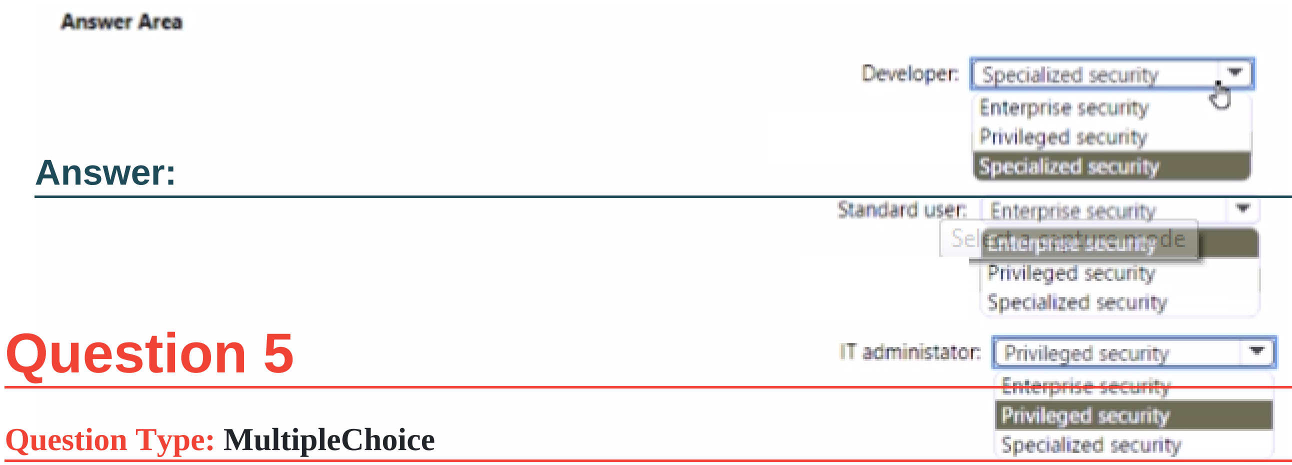
Question Type: **Hotspot**

You are planning the security levels for a security access strategy.

You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security level should you configure for each job role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Developer: Specialized security

Standard user: Enterprise security

IT administator: Privileged security

Answer:

Question 5

Question Type: **MultipleChoice**

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online. SharePoint Online, and Teams m near-real-lime (NRT) in response to the following Azure AD events:

* A user account is disabled or deleted

* The password of a user is changed or reset.

* All the refresh tokens for a user are revoked

* Multi-factor authentication (MFA) is enabled for a user

Which two features should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

Options:

A- continuous access evaluation

B- a sign-in risk policy

C- Azure AD Privileged Identity Management (PIM)

D- Conditional Access

E- Azure AD Application Proxy

Answer:

A, D

Question 6

Question Type: MultipleChoice

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised administrator account cannot be used to delete the backups

What should you do?

Options:

A- From a Recovery Services vault generate a security PIN for critical operations.

B- From Azure Backup, configure multi-user authorization by using Resource Guard.

C- From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault

D- From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

Answer:

B

Question 7

Question Type: **MultipleChoice**

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

Options:

A- Disable Microsoft OneDnve sync and Exchange ActiveSync.

B- Recover files to a cleaned computer or device.

C- Contact law enforcement.

D- From Microsoft Defender for Endpoint perform a security scan.

Answer:

A

Question 8

Question Type: **MultipleChoice**

You have an Azure AD tenant that syncs with an Active Directory Domain Services {AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators group on the Windows computers.

You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised.

What should you include in the recommendation?

Options:

A- Local Administrator Password Solution (LAPS)

B- Privileged Access Workstations (PAWs)

C- Azure AD Privileged Identity Management (PIM)

D- Azure AD identity Protection

Answer:

A