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 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. app registrations in Azure AD

B. application control policies in Microsoft Defender for Endpoint

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure AD Conditional Access App Control policies

Correct Answer: B

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.

Incorrect:

Not C: A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are

considered for each cloud application. Each increase is compared to the normal usage pattern of the application as learned from past usage. The most extreme increases trigger security alerts.

Reference:

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

QUESTION 2

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 groups 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?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

Correct Answer: A

Microsoft\\'s "Local Administrator Password Solution" (LAPS) provides management of local administrator account passwords for domain-joined computers. Passwords are randomized and stored in Active Directory (AD), protected by ACLs, so only eligible users can read it or request its reset.

Microsoft LAPS is short for Microsoft Local Administrator Password Solution. When installed and enabled on domain-joined computers it takes over the management of passwords of local accounts. Passwords are automatically changed to random characters that meet the domain\\'s password policy requirements at a frequency that you define through Group Policy.

The passwords are stored in a protected “confidential” attribute on the Computer object in AD. Unlike most other attributes which can be read by all domain users by default, the confidential attributes require extra privileges to be granted in order to read them, thus securing the managed passwords.

Incorrect: Not B: Integrate on-premises Active Directory domains with Azure Active Directory Validate security configuration and policy, Actively monitor Azure AD for signs of suspicious activity

Consider using Azure AD Premium P2 edition, which includes Azure AD Identity Protection. Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised. For example, it can detect potentially unusual activity such as irregular sign-in activities, sign-ins from unknown sources or from IP addresses with suspicious activity, or sign-ins from devices that may be infected. Identity Protection uses this data to generate reports and alerts that enable you to investigate these risk events and take appropriate action.

Not C: Azure AD PIM is a service in Azure AD that enables you to manage, control, and monitor access to resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Not D: Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides very strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket.

Reference: https://craighays.com/microsoft-laps/ https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

QUESTION 3

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.

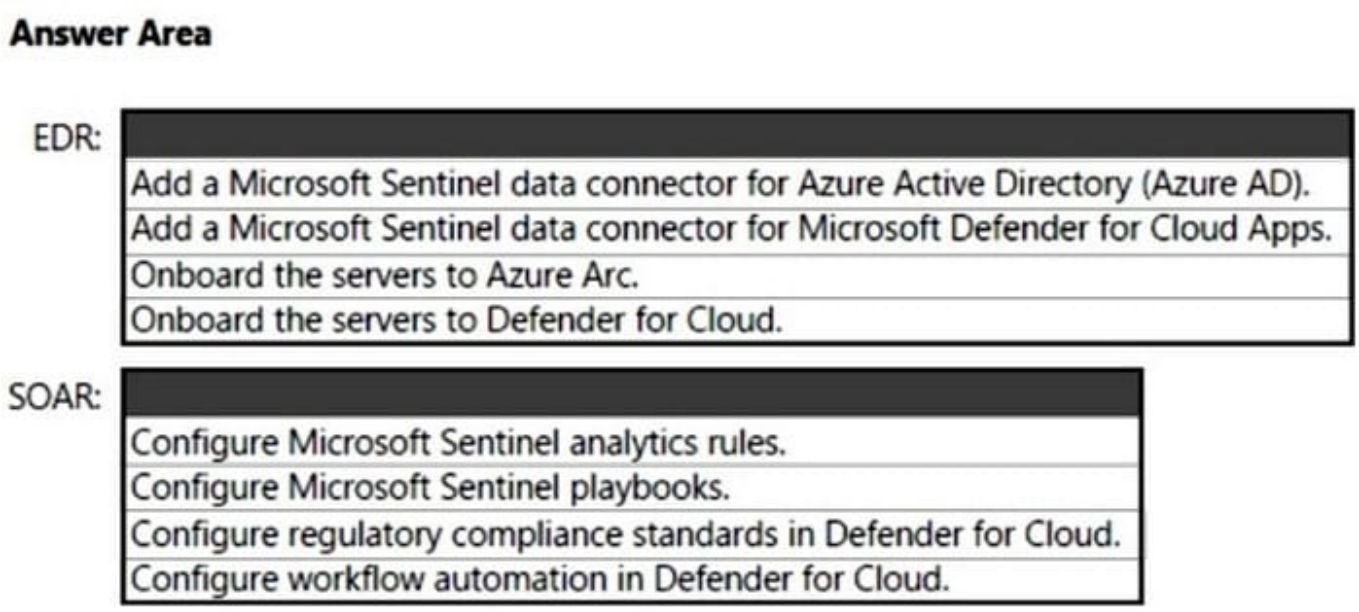
You plan to deploy Azure virtual machines that will run Windows Server.

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.

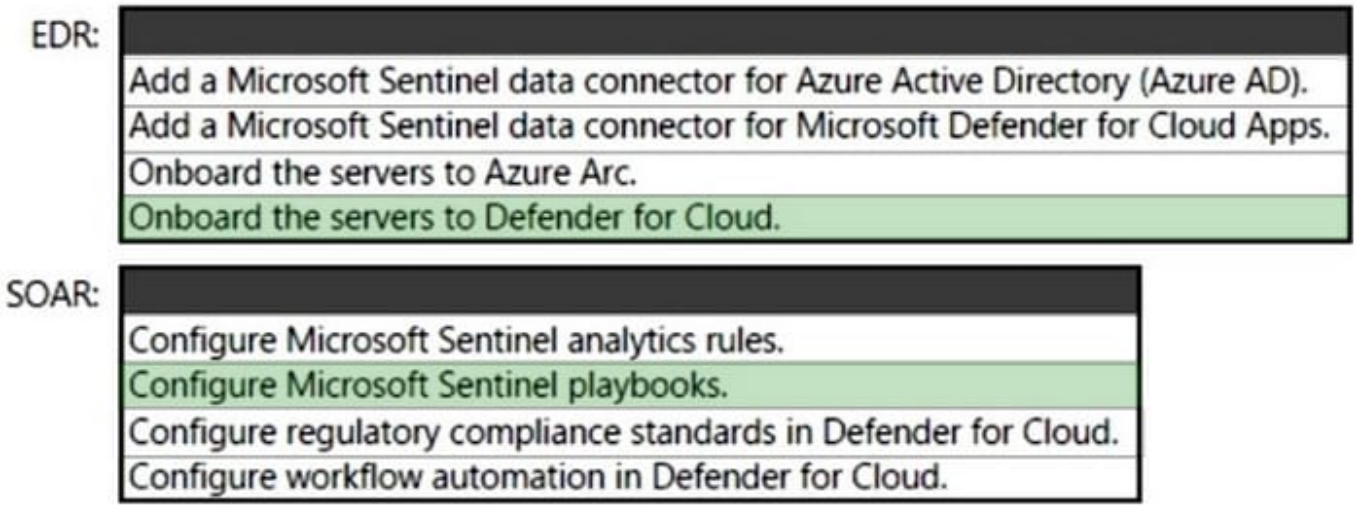
NOTE: Each correct selection is worth one point.

Hot Area:



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 4

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two solutions should you include in the design to ensure that preventative controls are implemented to increase the secure score? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Web Application Firewall (WAF)

B. Azure AD Privileged Identity Management (PIM)

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

Correct Answer: BC

B: Azure identity and access for landing zones, Privileged Identity Management (PIM)

Use Azure AD Privileged Identity Management (PIM) to establish zero-trust and least privilege access. Map your organization\\'s roles to the minimum access levels needed. Azure AD PIM can use Azure native tools, extend current tools and

processes, or use both current and native tools as needed.

Azure identity and access for landing zones, Design recommendations include:

*

(B) Use Azure AD managed identities for Azure resources to avoid credential-based authentication. Many security breaches of public cloud resources originate with credential theft embedded in code or other text. Enforcing managed identities for programmatic access greatly reduces the risk of credential theft.

*

Etc.

C: Improve landing zone security, onboard Microsoft Sentinel You can enable Microsoft Sentinel, and then set up data connectors to monitor and protect your environment. After you connect your data sources using data connectors, you choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.

Note: Landing zone security best practices

The following list of reference architectures and best practices provides examples of ways to improve landing zone security:

Microsoft Defender for Cloud: Onboard a subscription to Defender for Cloud.

Microsoft Sentinel: Onboard to Microsoft Sentinel to provide a security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Secure network architecture: Reference architecture for implementing a perimeter network and secure network

architecture.

Identity management and access control: Series of best practices for implementing identity and access to secure a landing zone in Azure.

Network security practices: Provides additional best practices for securing the network.

Operational security provides best practices for increasing operational security in Azure.

The Security Baseline discipline: Example of developing a governance-driven security baseline to enforce security requirements.

Incorrect:

Not E: Implementing alerts is not a preventive measure.

Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

QUESTION 5

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. unit testing

B. penetration testing

C. dependency checks

D. threat modeling

Correct Answer: B

Dynamic application security testing (DAST)

In a classical waterfall development model, security was typically introduced at the last step, right before going to production. One of the most popular security approaches is penetration testing or pen testing. Penetration testing lets a team

look at the application from a black-box security perspective, as in, closest to an attacker mindset.

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-devops-security

Latest SC-100 Dumps SC-100 Practice Test SC-100 Braindumps