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.pass4itsure.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 uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.

What should you include in the recommendation?

A. custom roles in Azure Pipelines

B. branch policies in Azure Repos

C. Azure policies

D. custom Azure roles

Correct Answer: B

Explanation:

Securing Azure Pipelines

YAML pipelines offer the best security for your Azure Pipelines. In contrast to classic build and release pipelines, YAML pipelines:

*

Can be code reviewed. YAML pipelines are no different from any other piece of code. You can prevent malicious actors from introducing malicious steps in your pipelines by enforcing the use of Pull Requests to merge changes. Branch policies make it easy for you to set this up.

*

Etc.

Reference: https://learn.microsoft.com/en-us/azure/devops/pipelines/security/overview

QUESTION 2

Reference: https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.

Note:

Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.

Recommendations:

-Internet-facing virtual machines should be protected with network security groups

-

Management ports of virtual machines should be protected with just-in-time network access control

-

Management ports should be closed on your virtual machines Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 3

DRAG DROP

Your company wants to optimize ransomware incident investigations.

You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.

Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

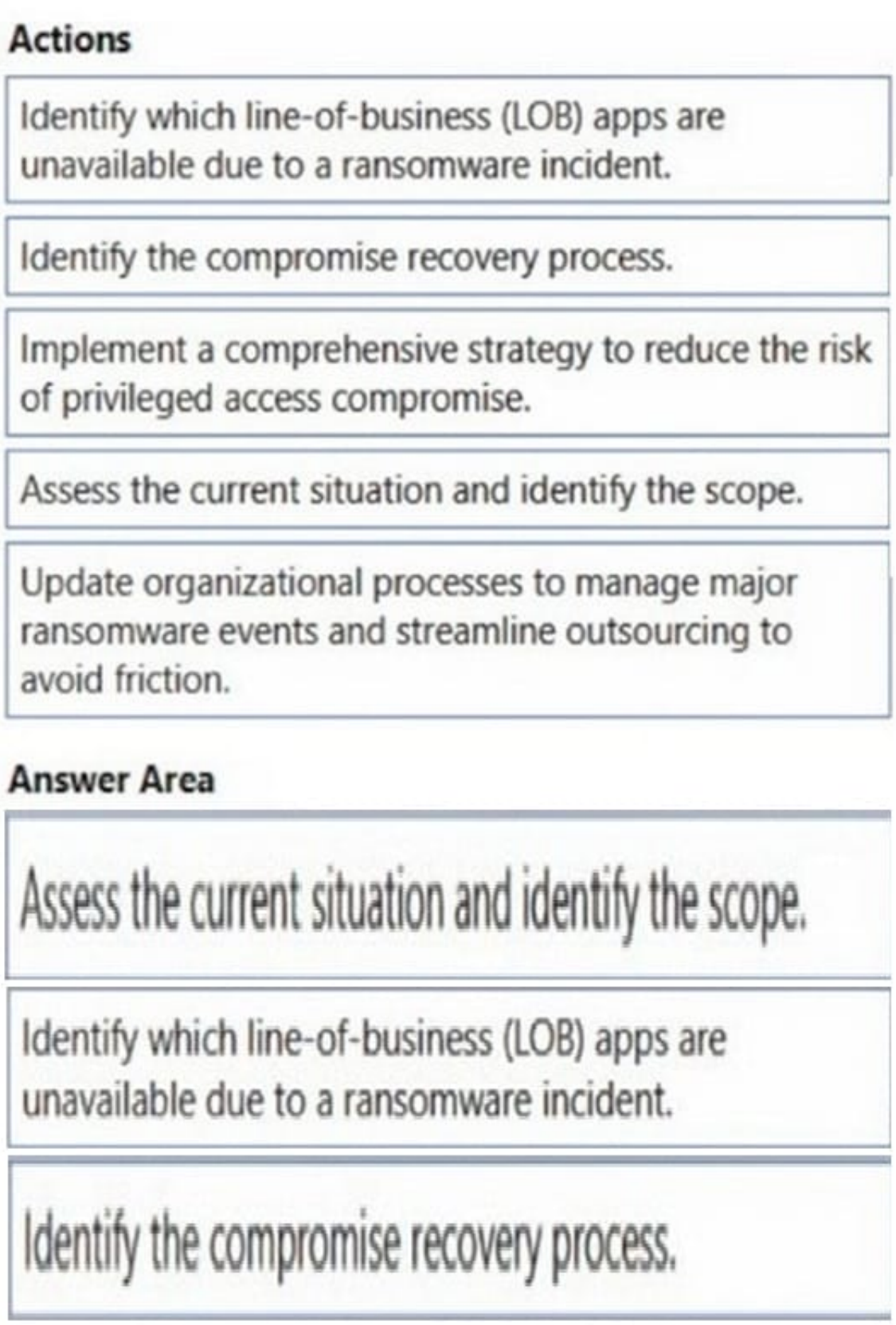
Select and Place:

Actions

- Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.
- Identify the compromise recovery process.
- Implement a comprehensive strategy to reduce the risk of privileged access compromise.
- Assess the current situation and identify the scope.
- Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

Answer Area

Correct Answer:



Step 1: Assess the current situation and identify the scope.

The DART approach to conducting ransomware incident investigations

You should make every effort to determine how the adversary gained access to your assets so that vulnerabilities can be remediated. Otherwise, it is highly likely that the same type of attack will take place again in the future. In some cases,

the threat actor takes steps to cover their tracks and destroy evidence, so it is possible that the entire chain of events may not be evident.

The following are three key steps in DART ransomware investigations:

1. Assess the current situation Understand the scope

What initially made you aware of a ransomware attack?

What time/date did you first learn of the incident?

What logs are available and is there any indication that the actor is currently accessing systems?

Step 2: Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.

2. Identify the affected line-of-business (LOB) apps Get systems back online

Does the application require an identity?

Are backups of the application, configuration, and data available?

Are the content and integrity of backups regularly verified using a restore exercise?

Step 3: Identify the compromise recovery process.

3. Determine the compromise recovery (CR) process Remove attacker control from the environment

Reference: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

QUESTION 4

HOTSPOT

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation.

You need to recommend a security posture management solution for the following components:

1.

Azure IoT Edge devices

2.

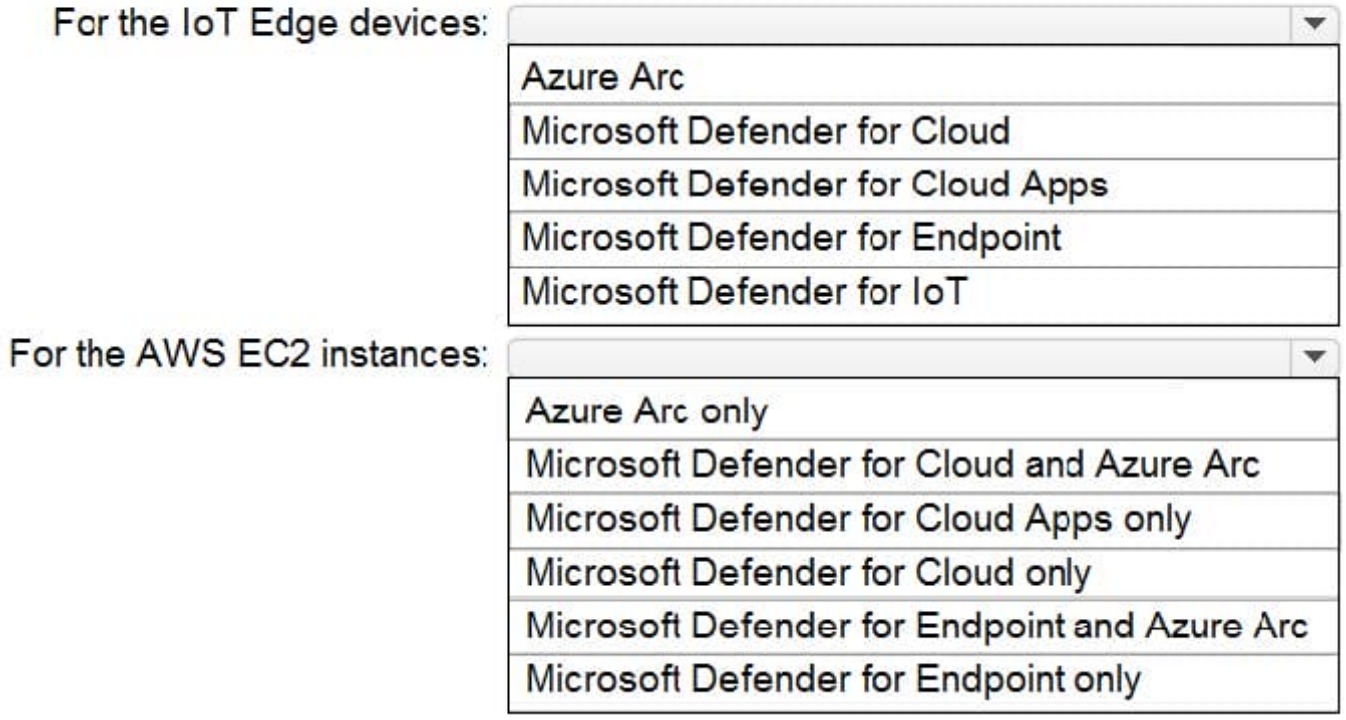
AWS EC2 instances

Which services should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

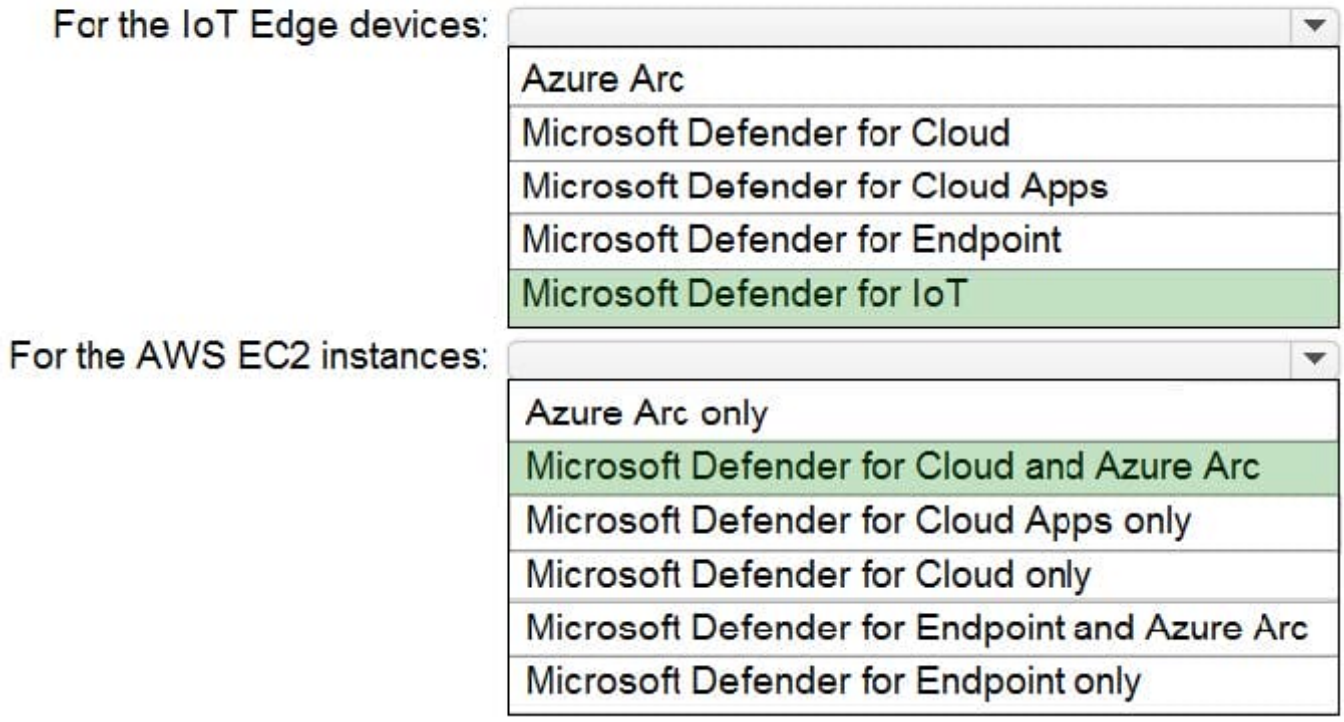
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Microsoft Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Azure IoT Edge provides powerful capabilities to manage and perform business workflows at the edge. The key part that IoT Edge plays in IoT environments make it particularly attractive for malicious actors.

Defender for IoT azureiotsecurity provides a comprehensive security solution for your IoT Edge devices. Defender for IoT module collects, aggregates and analyzes raw security data from your Operating System and container system into

actionable security recommendations and alerts.

Box 2: Microsoft Defender for Cloud and Azure Arc

Microsoft Defender for Cloud provides the following features in the CSPM (Cloud Security Posture Management) category in the multi-cloud scenario for AWS. Take into account that some of them require Defender plan to be enabled (such

as Regulatory Compliance):

*

Detection of security misconfigurations

*

Single view showing Security Center recommendations and AWS Security Hub findings

*

Incorporation of AWS resources into Security Center\\'s secure score calculations

*

Regulatory compliance assessments of AWS resources

Security Center uses Azure Arc to deploy the Log Analytics agent to AWS instances.

Incorrect: AWS EC2 Microsoft Defender for Cloud Apps Amazon Web Services is an IaaS provider that enables your organization to host and manage their entire workloads in the cloud. Along with the benefits of leveraging infrastructure in the cloud, your organization\\'s most critical assets may be exposed to threats. Exposed assets include storage instances with potentially sensitive information, compute resources that operate some of your most critical applications, ports, and virtual private networks that enable access to your organization.

Connecting AWS to Defender for Cloud Apps helps you secure your assets and detect potential threats by monitoring administrative and sign-in activities, notifying on possible brute force attacks, malicious use of a privileged user account, unusual deletions of VMs, and publicly exposed storage buckets.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/security-edge-architecture https://samilamppu.com/2021/11/04/multi-cloud-security-posture-management-in-microsoft-defender-for-cloud/

QUESTION 5

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft 365 subscription, and an Azure subscription.

The company\\'s on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

1.

Prevent the remote users from accessing any other resources on the network.

2.

Support Azure Active Directory (Azure AD) Conditional Access.

3.

Simplify the end-user experience. What should you include in the recommendation?

A. Azure AD Application Proxy

B. web content filtering in Microsoft Defender for Endpoint

C. Microsoft Tunnel

D. Azure Virtual WAN

Correct Answer: A

Azure Active Directory\\'s Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal

application portal.

Azure AD Application Proxy is:

Secure. On-premises applications can use Azure\\'s authorization controls and security analytics. For example, on-premises applications can use Conditional Access and two-step verification. Application Proxy doesn\\'t require you to open

inbound connections through your firewall.

Simple to use. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don\\'t need to change or update your applications to work with Application Proxy.

Incorrect:

Not D: Azure Virtual WAN

Azure Virtual WAN is for end users, not for applications.

Note: Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:

Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).

Site-to-site VPN connectivity.

Remote user VPN connectivity (point-to-site).

Private connectivity (ExpressRoute).

Intra-cloud connectivity (transitive connectivity for virtual networks).

VPN ExpressRoute inter-connectivity.

Routing, Azure Firewall, and encryption for private connectivity.

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