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 design cloud-based software as a service (SaaS) solutions.

You need to recommend a recovery solution for ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend doing first?

A. Develop a privileged identity strategy.

B. Implement data protection.

C. Develop a privileged access strategy.

D. Prepare a recovery plan.

Correct Answer: D

Recommend a ransomware strategy by using Microsoft Security Best Practices The three important phases of ransomware protection are:

*

create a recovery plan

*

limit the scope of damage

*

harden key infrastructure elements

Plan for ransomware protection and extortion-based attacks Phase 1 of ransomware protection is to develop a recovery plan. The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom. While attackers in control of your organization have a variety of ways to pressure you into paying, the demands

primarily focus on two categories:

Pay to regain access

Pay to avoid disclosure

Reference:

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-for-ransomware-protection-extortion-based-attacks

QUESTION 2

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

QUESTION 3

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All on-premises servers in the perimeter network are prevented from connecting directly to the internet.

The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend solutions to meet the following requirements:

1.

Ensure that the security operations team can access the security logs and the operation logs.

2.

Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network. Which two solutions should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a custom collector that uses the Log Analytics agent

B. the Azure Monitor agent

C. resource-based role-based access control (RBAC)

D. Azure Active Directory (Azure AD) Conditional Access policies

Correct Answer: BC

A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data

during collection to individual fields.

You can connect your data sources to Microsoft Sentinel using custom log formats.

C: Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel. The different roles give you fine-grained control over what Microsoft Sentinel users can see and do. Azure

roles can be assigned in the Microsoft Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel inherits.

Incorrect:

A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.

You can connect your data sources to Microsoft Sentinel using custom log formats.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview https://docs.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG https://docs.microsoft.com/en-us/azure/sentinel/roles

---

QUESTION 4

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

You are designing a Microsoft deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.

What should you recommend using in Microsoft Sentinel?

A. playbooks

B. workbooks

C. notebooks

D. threat intelligence

Correct Answer: B

After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what\\'s happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/get-visibility

QUESTION 5

Your company has an Azure subscription that uses Azure Storage.

The company plans to share specific blobs with vendors.

You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be time-limited.

What should you include in the recommendation?

A. Configure private link connections.

B. Configure encryption by using customer-managed keys (CMKs).

C. Share the connection string of the access key.

D. Create shared access signatures (SAS).

Correct Answer: D

A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:

What resources the client may access.

What permissions they have to those resources.

How long the SAS is valid.

Types of shared access signatures

Azure Storage supports three types of shared access signatures:

User delegation SAS

Service SAS

Account SAS

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

Latest SC-100 Dumps SC-100 Exam Questions SC-100 Braindumps