SC-100$^{Q\&As}$

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

QUESTION 1

You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.

Which two services should you leverage in the strategy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. access reviews in Azure AD

C. Microsoft Defender for Cloud

D. Microsoft Defender for Cloud Apps

E. Microsoft Defender for Endpoint

Correct Answer: BD

Scenario: Litware identifies the following application security requirements:

Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

B: Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User\\'s access can be reviewed on a regular basis to make sure only the right people have continued access.

D: The Defender for Cloud Apps framework Discover and control the use of Shadow IT: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.

Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real time across all your cloud apps.

Etc.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview
https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

QUESTION 2

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 3

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 4

You are designing the security standards for a new Azure environment.

You need to design a privileged identity strategy based on the Zero Trust model.

Which framework should you follow to create the design?

A. Enhanced Security Admin Environment (ESAE)

B. Microsoft Security Development Lifecycle (SDL)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)

Correct Answer: C

RaMP initiatives for Zero Trust.

To rapidly adopt Zero Trust in your organization, RaMP offers technical deployment guidance organized in these initiatives.

In particular, meet these deployment objectives to protect your privileged identities with Zero Trust.

1.

Deploy secured privileged access to protect administrative user accounts.

2.

Deploy Azure AD Privileged Identity Management (PIM) for a time-bound, just-in-time approval process for the use of privileged user accounts.

Note 1: RaMP guidance takes a project management and checklist approach:

* User access and productivity

1. Explicitly validate trust for all access requests Identities Endpoints (devices) Apps Network

* Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

* Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

Reduce manual effort

Note 2: As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and

gives you a set of deployment paths to more quickly implement key layers of protection.

By providing a suggested mapping of key stakeholders, implementers, and their accountabilities, you can more quickly organize an internal project and define the tasks and owners to drive them to conclusion.

By providing a checklist of deployment objectives and implementation steps, you can see the bigger picture of infrastructure requirements and track your progress.

Incorrect:

Not B: Enhanced Security Admin Environment (ESAE)

The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is an approach to provide a secure environment for Windows Server Active Directory (AD) administrators.

Microsoft\\'s recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP) guidance as the default recommended approach for securing privileged users.

The ESAE hardened administrative forest pattern (on-prem or cloud-based) is now considered a custom configuration suitable only for exception cases listed below.

What are the valid ESAE use cases?

While not a mainstream recommendation, this architectural pattern is valid in a limited set of scenarios.

In these exception cases, the organization must accept the increased technical complexity and operational costs of the solution. The organization must have a sophisticated security program to measure risk, monitor risk, and apply consistent

operational rigor to the usage and maintenance of the ESAE implementation.

Example scenarios include:

Isolated on-premises environments - where cloud services are unavailable such as offline research laboratories, critical infrastructure or utilities, disconnected operational technology (OT) environments such as Supervisory control and data

acquisition (SCADA) / Industrial Control Systems (ICS), and public sector customers that are fully reliant on on-premises technology.

Highly regulated environments – industry or government regulation may specifically require an administrative forest configuration.

High level security assurance is mandated - organizations with low risk tolerance that are willing to accept the increased complexity and operational cost of the solution.

Reference: https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

https://docs.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities

https://docs.microsoft.com/en-us/security/compass/esae-retirement

QUESTION 5

You have Windows 11 devices and Microsoft 365 E5 licenses.

You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.

What should you include in the recommendation?

A. Microsoft Endpoint Manager

B. Compliance Manager

C. Microsoft Defender for Cloud Apps

D. Microsoft Defender for Endpoint

Correct Answer: D

Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not

malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.

Note: Turn on web content filtering

From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering. Switch the toggle to On and Save preferences.

Configure web content filtering policies

Web content filtering policies specify which site categories are blocked on which device groups. To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering