SC-900^{Q&As}

SC-900^Q&As

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sc-900.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Define the perimeter by physical locations.

B. Use identity as the primary security boundary.

C. Always verify the permissions of a user explicitly.

D. Always assume that the user system can be breached.

E. Use the network as the primary security boundary.

Correct Answer: BCD

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

QUESTION 2

You have an Azure subscription that contains a Log Analytics workspace.

You need to onboard Microsoft Sentinel.

What should you do first?

A. Create a hunting query.

B. Correlate alerts into incidents.

C. Connect to your security sources.

D. Create a custom detection rule.

Correct Answer: C

Pre-deployment activities

Before deploying Microsoft Sentinel, we recommend taking the following steps to help focus your deployment on providing maximum value, as soon as possible.

*

 Determine which data sources you need and the data size requirements to help you accurately project your deployment\\\'s budget and timeline.

You might determine this information during your business use case review, or by evaluating a current SIEM that you already have in place. If you already have a SIEM in place, analyze your data to understand which data sources provide the most value and should be ingested into Microsoft Sentinel.

*

 Etc.

Reference: https://learn.microsoft.com/en-us/azure/sentinel/prerequisites

QUESTION 3

What can you protect by using the information protection solution in the Microsoft 365 compliance center?

A. computers from zero-day exploits

B. users from phishing attempts

C. files from malware and viruses

D. sensitive data from being exposed to unauthorized users

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

QUESTION 4

In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Plan

B. Manage

C. Adopt

D. Govern

E. Define Strategy

Correct Answer: AE

Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview

QUESTION 5

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point

Hot Area:

	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	○	○
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	○	○
Hunting provides you with the ability to identify security threats before an alert is triggered.	○	○

Correct Answer:

	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	○	●
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	●	○
Hunting provides you with the ability to identify security threats before an alert is triggered.	●	○

Box 1: No

Microsoft Sentinel data connectors are available for non-Microsoft services like Amazon Web Services.

Box 2: Yes

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the

Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also

comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Box 3: Yes

To help security analysts look proactively for new anomalies that weren\'t detected by your security apps or even by your scheduled analytics rules, Microsoft Sentinel\'s built-in hunting queries guide you into asking the right questions to find

issues in the data you already have on your network.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference

https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data

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

SC-900 VCE Dumps   SC-900 Practice Test   SC-900 Exam Questions