

Quiz 2026 Microsoft Perfect SC-200: Exam Microsoft Security Operations Analyst Learning



2026 Latest TroytecDumps SC-200 PDF Dumps and SC-200 Exam Engine Free Share: <https://drive.google.com/open?id=1H2uYcME3gbtqiFmK6IMladw8ECJ0YfEP>

Once you get the Microsoft SC-200 certificate, you can quickly quit your current job and then change a desirable job. The Microsoft SC-200 certificate can prove that you are a competent person. So it is easy for you to pass the interview and get the job. The assistance of our SC-200 practice quiz will change your life a lot.

Microsoft SC-200 exam covers a wide range of topics, including threat protection, vulnerability management, incident response, and compliance. Microsoft Security Operations Analyst certification exam is designed to test a candidate's ability to identify, assess, and respond to security threats in real-time. SC-200 Exam consists of multiple-choice questions that test a candidate's knowledge and skills in various areas of cybersecurity. SC-200 exam duration is 180 minutes, and the candidate must score at least 700 out of 1000 to pass the exam.

>> Exam SC-200 Learning <<

TroytecDumps Microsoft SC-200 Practice Exam material

When you are struggling with those troublesome reference books; when you feel helpless to be productive during the process of preparing SC-200 exams; when you have difficulty in making full use of your sporadic time and avoiding procrastination. It is time for you to realize the importance of our SC-200 Test Prep, which can help you solve these annoyance and obtain a SC-200 certificate in a more efficient and productive way. Not only will you be able to pass any SC-200 test, but will gets higher score, if you choose our SC-200 study materials.

Microsoft SC-200 certification exam covers a wide range of security topics including security operations management, threat intelligence, incident response, risk management, compliance, and data privacy. Candidates are required to demonstrate their ability to identify security risks, analyze security data, implement security solutions, and manage security incidents using Microsoft technologies. With the growing demand for cybersecurity professionals, obtaining the Microsoft SC-200 Certification can enhance your career prospects and help you stand out in the job market.

Microsoft Security Operations Analyst Sample Questions (Q159-Q164):

NEW QUESTION # 159

You have a Microsoft 365 subscription that contains three users named User1, User2 and User3 and the resources shown in the following table.

You have a Microsoft Defender XDR detection rule named Rule1 that has the following configurations:

- * Scope: DevGroup1
- * File hash: File1.exe
- * Actions
 - o Devices: Collect investigation package
 - o User: Mark as compromised
 - o Files: Block

Each user attempts to run File1.exe on their device.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

NEW QUESTION # 160

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833>

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

NEW QUESTION # 161

You have an Azure subscription that contains 100 Linux virtual machines.

You need to configure Microsoft Sentinel to collect event logs from the virtual machines.

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

Answer:

Explanation:

Explanation:

To collect event logs from Linux virtual machines in Microsoft Sentinel, the data ingestion path must be correctly configured through Azure Monitor (Log Analytics) and Sentinel connectors. The correct order of actions is as follows:

1## Add Microsoft Sentinel to a workspace:

Sentinel requires a Log Analytics workspace as its data foundation. You must first enable Microsoft Sentinel on a workspace by selecting Microsoft Sentinel # Add # Select workspace. This step prepares the workspace to receive and analyze security data.

2## Add a Syslog connector to the workspace:

Linux systems send event data through Syslog. You must enable the Syslog connector within the Sentinel workspace. The connector defines which Syslog facilities and severities should be collected and ingested into Sentinel. It acts as the integration bridge between the Linux hosts and Sentinel's analytics engine.

3## Install the Log Analytics agent for Linux on the virtual machines:

To forward the logs, each Linux virtual machine needs the Log Analytics agent (OMS agent). This agent collects the configured Syslog and performance data and sends it to the connected Log Analytics workspace.

This sequence ensures proper setup for Linux log ingestion: Sentinel is first activated, then the Syslog data source is configured, and finally, agents are deployed to gather and transmit the logs.

NEW QUESTION # 162

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

2026 Latest TroytecDumps SC-200 PDF Dumps and SC-200 Exam Engine Free Share: <https://drive.google.com/open?id=1H2uYcME3gbtqiFmK6IMladw8ECJ0YfEP>