100% Pass 2026 Microsoft SC-200: Microsoft Security Operations Analyst–High-quality Reliable Test Cost

What's more, part of that ExamsLabs SC-200 dumps now are free: https://drive.google.com/open?id=11jboBcmKk94jQq_FrJfZKnq4b9QE9Acs

ExamsLabs is a website to achieve dreams of many IT people. ExamsLabs provide candidates participating in the IT certification exams the information they want to help them pass the exam. Do you still worry about passing Microsoft certification SC-200 exam? Have you thought about purchasing an Microsoft certification SC-200 exam counseling sessions to assist you? ExamsLabs can provide you with this convenience. ExamsLabs's training materials can help you pass the certification exam. ExamsLabs's exercises are almost similar to real exams. With ExamsLabs's accurate Microsoft Certification SC-200 Exam practice questions and answers, you can pass Microsoft certification SC-200 exam with a high score.

Microsoft SC-200 is an exam designed for security operations analysts who want to validate their skills and knowledge in identifying, investigating, and responding to security threats in a Microsoft environment. Microsoft Security Operations Analyst certification exam is a part of the Microsoft Certified: Security Operations Analyst Associate certification path and is intended for individuals who work with Microsoft security solutions on a regular basis.

>> Reliable SC-200 Test Cost <<

SC-200 test dumps & SC-200 pass rate & SC-200 Test king

It will make them scrutinize how our formats work and what we offer them, for example, the form and pattern of Microsoft SC-200 exam dumps, and their relevant and updated answers. It is convenient for our consumers to check Microsoft SC-200 Exam Questions free of charge before purchasing the Microsoft SC-200 practice exam.

Microsoft Security Operations Analyst Sample Questions (Q18-Q23):

NEW QUESTION # 18
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.
You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector. The attacker performs the tactics shown the following table.
You need to search for malicious activities in your organization.
Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

- A. Taclic1. Tac1ic2. andTactic3
- B. Tac1ic2 and Tactic3 only
- C. Tactic2 only
- D. Tactic1 and Tactic2 only

Answer: A

NEW QUESTION # 19
You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION # 20
You have the following advanced hunting query in Microsoft 365 Defender.
You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Add | order by Timestamp to the query.
- B. Create a suppression rule.
- C. Create a detection rule.
- D. Add DeviceId and ReportId to the output of the query.
- E. Block DeviceProcessEvents with DeviceNetworkEvents.

Answer: C,D

Explanation:
In Microsoft 365 Defender advanced hunting, if you want to automatically receive alerts based on a KQL query-such as detecting when a process disables System Restore-you must convert that query into a custom detection rule. According to Microsoft's official documentation, custom detection rules "run hunting queries on a schedule and create alerts and incidents when results are found." In order for the detection rule to function properly and correlate results across devices and incidents, the query must output DeviceId and ReportId. These fields are mandatory for any advanced hunting query that you want to convert into a detection rule because they uniquely identify the device and event instance. Without them, the rule cannot properly generate correlated alerts.
Therefore:
* Create a detection rule (A) - ensures the query runs automatically and alerts are generated.
* Add DeviceId and ReportId (E) - required for detection rule creation and accurate device/event correlation.
Other options are incorrect:
* Suppression rule (B) filters alerts, not generate them.
* Order by Timestamp (C) is optional for display, not alerting.
* DeviceNetworkEvents (D) is unrelated to this process query.

NEW QUESTION # 21
You have an Azure subscription.
You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.
You need to configure storage for the workspace. The solution must meet the following requirements:
* Minimize costs for daily ingested data.
* Maximize the data retention period without incurring extra costs.
What should you do for each requirement? To answer, select the appropriate options in the answer are a. NOTE Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION # 22

You have an Azure subscription that contains 50 virtual machines.
You plan to deploy Microsoft [Defender for Cloud.
You need to enable agentless scanning for 40 virtual machines. The solution must create disk snapshots of the virtual machines and perform out-of-band analysis of the snapshots.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:

NEW QUESTION # 23
.....

The SC-200 torrent prep contains the real questions and simulation questions of various qualifying examinations. It is very worthy of study efficiently. Time is constant development, and proposition experts will set questions of real SC-200 exam continuously according to the progress of the society change tendency of proposition, and consciously highlight the hot issues and policy changes. In order to be able to better grasp the proposition thesis direction, the SC-200 study question focus on the latest content to help you pass the SC-200 exam.