Valid Exam SC-200 Registration & SC-200 Exam Dumps

P.S. Free 2026 Microsoft SC-200 dumps are available on Google Drive shared by SurePassExams: https://drive.google.com/open?id=1DlQyGGpvqXEUK9sck1RTimdJQoyqcqR8

If you free download the demos of the SC-200 exam questions, I believe you have a deeper understanding of our products, and we must also trust our SC-200 learning quiz. Our products can provide you with the high efficiency and high quality you need. Selecting our study materials is your rightful assistant with internationally recognized SC-200 Certification. What are you waiting for? Quickly use our SC-200 study materials.

Microsoft SC-200 Exam is an important certification for security professionals who work with Microsoft technologies. Achieving this certification demonstrates a strong understanding of security operations and the ability to implement effective security measures in a Microsoft environment. With the increasing demand for skilled security professionals, this certification can help boost career opportunities and salary potential.

>> Valid Exam SC-200 Registration <<

SC-200 Exam Dumps & SC-200 Test Guide

SC-200 practice exam enables applicants to practice time management, answer strategies, and all other elements of the final Microsoft Security Operations Analyst (SC-200) certification exam and can check their scores. The exhaustive report enrollment database allows students to evaluate their performance and prepare for the Microsoft Security Operations Analyst (SC-200) certification exam without further difficulty.

Microsoft Security Operations Analyst Sample Questions (Q410-Q415):

NEW QUESTION # 410
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.
How should you complete the query? 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/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

NEW QUESTION # 411
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
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.

a Microsoft 365 E5

Answer:

Explanation:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION # 412
You have a Microsoft Sentinel workspace that has a default data retention period of 30 days. The workspace contains two custom tables as shown in the following table.
Each table ingested two records per day during the past 365 days.
You build KQL statements for use in analytic rules as shown in the following table.
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 # 413
You are using the Microsoft 365 Defender portal to conduct an investigation into a multi-stage incident related to a suspected malicious document. After reviewing all the details, you have determined that the alert tied to the potentially malicious document is also related to another incident in your environment. However, the alert is not currently listed as a part of that second incident.
Your investigation into the alert is ongoing, as it is your investigation into the two related incidents.
You need to appropriately categorize the alert and ensure that it is associated with the second incident.
What two actions should you take in the Manage alert pane to fulfill this part of the investigation?
(Choose two)

- A. Select the Link alert to another incident option.
- B. Enter the Incident ID of the related incident in the Comment section.
- C. Set status to In progress
- D. Set classification to True alert
- E. Set status to New

Answer: A,C

Explanation:
The correct action to classify the alert would be to set the status to In progress. While the alert may seem to be legitimate as it is linked to another incident, until a final determination is reached, you should set the status to In progress to ensure that others know it is being worked on. Once a determination is reached, you can then change it to Resolved and select the appropriate classification (True alert or False alert).
The correct action to correlate the alert to the other incident would be to select the Link alert to another incident option. While ideally, the alert would automatically be included in both incidents that are not always the case. If you notice an alert that is not linked to an incident that it is clearly connected to, using the Link alert to another incident option ensures they are tied together.
You should not set the classification to True alert. While a point can be made that it seems this malicious file involved in multiple incidents is likely to be a True alert, you cannot yet make that determination. It is also not the time to classify it as a false alert. The best practice while continuing an investigation would be not to change the classification at all, which means leaving it as the default Not set classification.
You should not enter the Incident ID of the related incident in the Comment section. While this might be helpful from an administrative perspective, it creates no link to the other incident.
You should not set the status to New. This is the default status of any alert. The question specifically seeks to ensure your peers know the alert is being investigated, so setting (or leaving) the status as New would make it impossible to differentiate from other uninvestigated alerts.
All of the actions mentioned in the options can be found in the Manage alert pane, which can be reached via the Alerts tab in the

Incidents section of the Microsoft 365 Defender portal.
References:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- incidents?view=o365-worldwide

NEW QUESTION # 414
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
The security team at your company detects command and control (C2) agent traffic on the network. Agents communicate once every 50 hours.
You need to create a Microsoft Defender XDR custom detection rule that will identify compromised devices and establish a pattern of communication. The solution must meet the following requirements:
- Identify all the devices that have communicated during the past 14 days.
- Minimize how long it takes to identify the devices.
To what should you set the detection frequency for the rule?

- A. Every three hours
- B. Every 12 hours
- C. Every hour
- D. Every 24 hours

Answer: D

Explanation:
Every 24 hours - runs every 24 hours, checking data from the past 30 days
"Match the time filters in your query with the lookback duration. Results outside of the lookback duration are ignored."
https://learn.microsoft.com/en-us/defender-xdr/custom-detection-rules

NEW QUESTION # 415
.....

At the SurePassExams, we guarantee that our customers will receive the best possible Microsoft Security Operations Analyst (SC-200) study material to pass the Microsoft SC-200 certification exam with confidence. Joining this site for the SC-200 Exam Preparation would be the greatest solution to the problem of outdated material.

SC-200 Exam Dumps: https://www.surepassexams.com/SC-200-exam-bootcamp.html

- New SC-200 Exam Vce □ SC-200 Latest Braindumps Ppt □ Reliable SC-200 Study Materials □ Search for ➥ SC-200 □ and easily obtain a free download on 「 www.prepawayexam.com 」 □SC-200 Practice Engine
- 100% Pass Quiz Reliable Microsoft - SC-200 - Valid Exam Microsoft Security Operations Analyst Registration □ Search on ➽ www.pdfvce.com □ for 《 SC-200 》 to obtain exam materials for free download □Download SC-200 Free Dumps
- Latest SC-200 Dumps Free □ Latest SC-200 Dumps Free □ SC-200 Exam Tests □ Simply search for □ SC-200 □ for free download on ⇛ www.prepawayete.com ⇚ □SC-200 Examcollection Free Dumps
- Highly-Praised Microsoft Security Operations Analyst Qualification Question Helps You Pass the Microsoft Security Operations Analyst Exam Easily □ The page for free download of ✔ SC-200 □✔□ on ➤ www.pdfvce.com □ will open immediately □Trustworthy SC-200 Practice
- Latest SC-200 Demo □ SC-200 Study Demo □ SC-200 Online Lab Simulation □ Open □ www.testkingpass.com □ enter 「 SC-200 」 and obtain a free download □SC-200 Study Demo
- SC-200 Study Demo □ SC-200 Reliable Test Labs □ SC-200 Latest Learning Material □ Enter ➽ www.pdfvce.com □ and search for ▹ SC-200 ◃ to download for free □Download SC-200 Free Dumps
- SC-200 Valid Exam Practice ☑ SC-200 Study Demo □ New SC-200 Exam Vce □ Search for ➠ SC-200 □ and download it for free on " www.prep4away.com " website □Reliable SC-200 Study Materials
- SC-200 Reliable Test Labs □ Reliable SC-200 Study Materials □ SC-200 Valid Exam Practice □ Easily obtain free download of ➡ SC-200 □□□ by searching on 「 www.pdfvce.com 」 □SC-200 Test Passing Score
- Valid Exam SC-200 Registration Makes Passing Microsoft Security Operations Analyst Easier □ Search for □ SC-200 □ and download exam materials for free through ⇛ www.examcollectionpass.com ⇚ □SC-200 Test Passing Score
- 2026 Professional SC-200: Valid Exam Microsoft Security Operations Analyst Registration □ Open website ▹ www.pdfvce.com ◃ and search for （ SC-200 ） for free download □SC-200 Latest Learning Material

- SC-200 Valid Exam Practice □ SC-200 Test Simulator □ SC-200 Online Lab Simulation □ Download ✔ SC-200 □✔□ for free by simply searching on 《 www.examcollectionpass.com 》 □Test SC-200 Topics Pdf
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.wetrc.dripsprinklerirrigation.pk, learning.schrandersolutions.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

What's more, part of that SurePassExams SC-200 dumps now are free: https://drive.google.com/open?id=1DlQyGGpvqXEUK9sck1RTimdJQoyqcqR8