SC-200 Bestehen Sie Microsoft Security Operations Analyst! - mit höhere Effizienz und weniger Mühen

Außerdem sind jetzt einige Teile dieser EchteFrage SC-200 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1XRb_qd0_lECklh0c72Ljbz0Hjv58ISEE

Um die Interessen zu schützen, bietet unsere Website die online Prüfungen zur Microsoft SC-200 Zertifizierungsprüfung von EchteFrage, die von den erfahrungsreichen IT-Experten nach den Bedürfnissen bearbeitet werden. Sie werden Ihnen nicht nur helfen, die Microsoft SC-200 Prüfung zu bestehen und auch eine bessere Zukunft zu haben.

Alle Menschen haben ihre eigenes Ziel, aber wir haben ein gleiches Ziel, dass Sie Microsoft SC-200 Prüfung bestehen. Dieses Ziel zu erreichen ist vielleicht nur ein kleiner Schritt für Ihre Entwicklung im IT-Gebiet. Aber es ist der ganze Wert unserer Microsoft SC-200 Prüfungssoftware. Wir tun alles wir können, um die Prüfungsaufgaben zu erweitern. Und die Prüfungsunterlagen werden von unsere IT-Profis analysiert. Dadurch können Sie unbelastet und effizient benutzen. Um zu garantieren, dass die Microsoft SC-200 Unterlagen, die Sie benutzen, am neuesten ist, bieten wir einjährige kostenlose Aktualisierung.

>> SC-200 Online Prüfungen <<

SC-200 Online Tests & SC-200 PDF Testsoftware

Wenn Sie ein Pendler sind, wenn Sie die Microsoft SC-200 Prüfung so schnell wie möglich bestehen möchten, dass ist EchteFrage Ihre beste Wahl. Unser EchteFrage bietet Ihnen die Testfragen und Antworten von Microsoft SC-200, die von den IT-Experten durch Experimente und Praxis erhalten werden und über IT-Zertifizierungserfahrungen über 10 Jahre verfügt. Mit EchteFrage können Sie nicht nur Zeit sparen, sondern auch die Microsoft SC-200 Zertifizierungsprüfung leicht und züglich bestehen.

Um sich auf die Microsoft SC-200 Zertifizierungsprüfung vorzubereiten, müssen Kandidaten ein gutes Verständnis für die Grundlagen der Cybersicherheit haben, einschließlich Bedrohungsinformationen, Risikomanagement und Sicherheitsoperationen. Sie müssen auch Erfahrung mit Microsoft-Sicherheitstechnologien und -Tools haben. Microsoft bietet verschiedene Schulungsoptionen an, einschließlich instruktorgeleiteter Schulungen, Online-Kurse und selbstgesteuerten Lernmodulen, um Kandidaten bei der Vorbereitung auf die Prüfung zu unterstützen.

Microsoft Security Operations Analyst SC-200 Prüfungsfragen mit Lösungen

(Q175-Q180):

175. Frage
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You need to ensure that you can investigate threats by using data in the unified audit log of Microsoft Defender for Cloud Apps.
What should you configure first?

- A. the User enrichment settings
- B. the Automatic log upload settings
- C. the Microsoft 365 connector
- D. the Azure connector

Antwort: C

176. Frage
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
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.

Antwort:

Begründung:
1 - From Azure Sentinel, select Hunting.
2 - Filture by tactics.
3 - Select Run All Queries.

177. Frage
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Enable the Fusion rule.
- B. Add a playbook.
- C. Associate a playbook to the analytics rule that triggered the incident.
- D. Create a workbook.
- E. Enable Entity behavior analytics.

Antwort: C,E

Begründung:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

178. Frage
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.

Antwort:

Begründung:
Explanation:
Statements
Answer
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.
Yes
Both virtual machines have management ports exposed directly to the internet.
Yes
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four points.
Yes
In the Microsoft Defender for Cloud (Azure Security Center) screenshot, the Secure Score report shows several active security recommendations, including:
* "Restrict unauthorized network access" with a potential score increase of +9% (4 points) for 2 of 2 resources.
* "Secure management ports" with a potential score increase of +9% (4 points) for 1 of 2 resources.
These controls correspond to Defender for Cloud recommendations related to network security and exposure of management ports (RDP/SSH). The fact that both controls show "2 of 2 resources" or "1 of 2 resources" as unhealthy means both virtual machines currently have NSG or firewall rules that allow inbound access from "Any" or "Internet ranges," indicating open ports and insecure configurations.
According to Microsoft documentation ("Improve your Secure Score in Microsoft Defender for Cloud"), enabling Just-In-Time (JIT) VM access mitigates these findings by restricting inbound RDP/SSH access to approved users for limited time windows, thereby increasing the Secure Score. Each remediated recommendation increases the Secure Score by the number of points shown in the "Potential score increase" column (4 points in this case).
Because Azure Policy shows no assigned or conflicting policies, compliance enforcement is not yet active, confirming that the current exposure is due to lack of configuration rather than policy override.
Therefore:
* The two VMs have inbound Internet-accessible rules # Yes.
* They have management ports exposed # Yes.
* Enabling JIT network access would fix both recommendations, improving the Secure Score by 4 points
# Yes.

179. Frage
You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?

- A. notebooks in Azure Sentinel
- B. hunting queries in Azure Sentinel
- C. Microsoft Cloud App Security
- D. Azure Monitor

Antwort: A

Begründung:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

180. Frage
.....

◁ nach { SC-200 } und laden Sie es kostenlos herunter □SC-200 Zertifikatsdemo

- SC-200 Trainingsunterlagen □ SC-200 Zertifikatsfragen □ SC-200 German ⌨ □ de.fast2test.com □ ist die beste Webseite um den kostenlosen Download von ⇛ SC-200 ⇚ zu erhalten □SC-200 Testing Engine
- SC-200 Deutsche □ SC-200 Prüfung □ SC-200 Prüfung □ Suchen Sie jetzt auf □ www.itzert.com □ nach （ SC-200 ） und laden Sie es kostenlos herunter □SC-200 Ausbildungsressourcen
- SC-200 Dumps und Test Überprüfungen sind die beste Wahl für Ihre Microsoft SC-200 Testvorbereitung □ Suchen Sie auf 《 www.it-pruefung.com 》 nach kostenlosem Download von □ SC-200 □ □SC-200 Fragen Beantworten
- SC-200 Fragen Beantworten □ SC-200 Ausbildungsressourcen □ SC-200 Übungsmaterialien □ Öffnen Sie die Webseite ➤ www.itzert.com □ und suchen Sie nach kostenloser Download von 「 SC-200 」 □SC-200 Deutsche
- SC-200 Zertifikatsfragen □ SC-200 Zertifikatsfragen □ SC-200 Deutsch Prüfungsfragen □ Suchen Sie auf der Webseite 《 www.itzert.com 》 nach ➡ SC-200 □□□ und laden Sie es kostenlos herunter □SC-200 Simulationsfragen
- SC-200: Microsoft Security Operations Analyst Dumps - PassGuide SC-200 Examen □ URL kopieren { www.itzert.com } Öffnen und suchen Sie ➠ SC-200 □ Kostenloser Download □SC-200 Fragen Beantworten
- SC-200 Prüfungsressourcen: Microsoft Security Operations Analyst - SC-200 Reale Fragen □ Geben Sie ➥ www.zertpruefung.ch □ ein und suchen Sie nach kostenloser Download von ▸ SC-200 ◂ □SC-200 Tests
- SC-200 Prüfung □ SC-200 Simulationsfragen □ SC-200 Prüfung □ Öffnen Sie die Webseite [www.itzert.com] und suchen Sie nach kostenloser Download von □ SC-200 □ □SC-200 Deutsch Prüfung
- SC-200 Prüfungsressourcen: Microsoft Security Operations Analyst - SC-200 Reale Fragen □ Suchen Sie auf （ www.zertpruefung.ch ） nach □ SC-200 □ und erhalten Sie den kostenlosen Download mühelos □SC-200 Lerntipps
- matrixbreach.com, academy.cooplus.org, 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, 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, courses.adgrove.co, 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, 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, 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, Disposable vapes

Außerdem sind jetzt einige Teile dieser EchteFrage SC-200 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1XRb_qd0_lECklh0c72Ljbz0Hjv58ISEE