看到SC-200在線題庫意味著你已經通過了Microsoft Security Operations Analyst的一半

P.S. VCESoft在Google Drive上分享了免費的2026 Microsoft SC-200考試題庫：https://drive.google.com/open?id=1lbh7Q7Lf3ymZXl1Bnba9sfSpnkqolJng

現在IT行业競爭越來越激烈，通過Microsoft SC-200認證考試可以有效的帮助你在现在这个竞争激烈的IT行业中稳固和提升自己的地位。在我們VCESoft中你可以獲得關Microsoft SC-200認證考試的培訓工具。我們VCESoft的IT精英團隊會及時為你提供準確以及詳細的關Microsoft SC-200認證考試的培訓材料。通過我們VCESoft提供的學習材料以及考試練習題和答案，我們VCESoft能確保你第一次參加Microsoft SC-200认证考试時挑戰成功，而且不用花費大量時間和精力來準備考試。

微軟SC-200認證考試為時兩小時，共計40-60道題目，以多選和場景題為主調。考生將面臨現實場景，被要求選擇最佳的行動方案。考試在線進行，參考人員可在全球任何地點參加。考試通過後，考生將獲得微軟認證：安全運營分析師助理證書。

要成為Microsoft SC-200認證，候選人必須具備強大的Microsoft安全技術知識，包括Azure Sentinel、Microsoft Defender for Endpoint和Microsoft Cloud App Security。該考試包含多項選擇題、案例研究和實踐任務，測試候選人識別和響應各種安全事件的能力。成功的候選人需要展示他們的事件分類、調查潛在安全漏洞以及識別和實施適當的補救措施的能力。總的來說，Microsoft SC-200認證是安全分析師想要推進職業發展並展示對Microsoft安全技術專業知識的有價值的證書。

>> SC-200在線題庫 <<

Microsoft SC-200認證考試 - SC-200考題

VCESoft是一個對Microsoft SC-200 認證考試提供針對性培訓的網站。VCESoft也是一個不僅能使你的專業知識得到提升，而且能使你一次性通過Microsoft SC-200 認證考試的網站。VCESoft提供的培訓資料是由很多IT資深專家不斷利用自己的經驗和知識研究出來的，品質很好，準確性很高。一旦你選擇了我們VCESoft，不僅能夠幫你通過Microsoft SC-200 認證考試和鞏固自己的IT專業知識，還可以享用一年的免費售後更新服務。

最新的 Microsoft Certified: Security Operations Analyst Associate SC-200 免費考試真題 (Q294-Q299):

問題 #294
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
Enable and disable Azure Defender.
Apply security recommendations to resource.
The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

答案：

解題說明：
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

問題 #295
HOTSPOT
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.
Hot Area:

答案：

解題說明：
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide
Testlet 1
Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam.
You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.
Network Environment
Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure

subscription.
On-premises Environment
The on-premises network contains the computers shown in the following table.
Current problems
Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.
Planned Changes
Litware plans to implement the following changes:
* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by using Azure AD test user accounts.
Business Requirements
Litware identifies the following business requirements:
* The principle of least privilege must be used whenever possible.
* Costs must be minimized, as long as all other requirements are met.
* Logs collected by Log Analytics must provide a full audit trail of user activities.
* All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.
Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

問題 #296
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.

答案：

解題說明：
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

問題 #297
You are configuring Microsoft Cloud App Security.
You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.
You receive many alerts related to impossible travel and sign-ins from risky IP addresses.
You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.
You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Override automatic data enrichment.
- B. Increase the sensitivity level of the impossible travel anomaly detection policy.
- C. Add the IP addresses to the other address range category and add a tag.

- D. Create an activity policy that has an exclusion for the IP addresses.
- E. Add the IP addresses to the corporate address range category.

答案：A,C

問題 #298
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

答案：

解題說明：

問題 #299
.....

如果你正在準備 SC-200 考試，為 SC-200 認證做最後衝刺，又苦於沒有絕對權威的考試真題模擬。很多考生現在都用 Microsoft SC-200 考題作為參加SC-200 考試最快捷，最信任的方式。擺正好心態，認真閱讀准備好的 SC-200 考題，考試時心中不要慌，任何一場考試，都是與考生在進行心理戰的准備，遇到難的題目先不要去管，調整好心態准備應戰下一條題目。加上之前准備充足獲取 SC-200 認證應該是沒有問題的。

SC-200認證考試: https://www.vcesoft.com/SC-200-pdf.html

- 快速下載的SC-200在線題庫，保證幫助妳壹次性通過SC-200考試 □ ➤ www.newdumpspdf.com □上的□ SC-200 □免費下載只需搜尋最新SC-200題庫資源
- 分享最新版本的SC-200題庫 - 免費下載Microsoft Security Operations Analyst - SC-200擬真試題 □ 透過▸ www.newdumpspdf.com ◂輕鬆獲取➽ SC-200 □免費下載SC-200證照信息
- 分享最新版本的SC-200題庫 - 免費下載Microsoft Security Operations Analyst - SC-200擬真試題 ✔ （ www.pdfexamdumps.com ）上的免費下載□ SC-200 □頁面立即打開SC-200測試引擎
- SC-200熱門考題 □ SC-200考試題庫 □ SC-200證照指南 □ □ www.newdumpspdf.com □最新➥ SC-200 □ 問題集合SC-200證照
- 最受歡迎的SC-200在線題庫，Microsoft Microsoft Certified: Security Operations Analyst Associate認證SC-200考試題庫提供免費下載 □ ▸ tw.fast2test.com ◂提供免費（ SC-200 ）問題收集最新SC-200題庫資源
- SC-200考古題推薦 □ SC-200資訊 □ SC-200資訊 □ 到「 www.newdumpspdf.com 」搜索➽ SC-200 □輕鬆取得免費下載SC-200題庫更新
- SC-200證照指南 □ SC-200學習筆記 □ SC-200真題 □ 進入【 www.pdfexamdumps.com 】搜尋《 SC-200 》免費下載SC-200認證
- SC-200考古題推薦 □ SC-200認證 □ SC-200權威認證 □ [www.newdumpspdf.com]上搜索【 SC-200 】輕鬆獲取免費下載SC-200熱門考古題
- 信任www.newdumpspdf.com中的授權的SC-200在線題庫是通過Microsoft Security Operations Analyst的有效方式 □ □ 到《 www.newdumpspdf.com 》搜索「 SC-200 」輕鬆取得免費下載SC-200真題
- SC-200權威認證 □ SC-200下載 □ SC-200考試題庫 □ ➠ www.newdumpspdf.com □上的免費下載✔ SC-200 □✔□頁面立即打開SC-200資訊
- SC-200證照指南 □ SC-200題庫更新 □ SC-200證照指南 □ 《 www.newdumpspdf.com 》上搜索【 SC-200 】輕鬆獲取免費下載SC-200權威認證
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.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, 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.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. VCESoft在Google Drive上分享了免費的2026 Microsoft SC-200考試題庫：https://drive.google.com/open?id=1lbh7Q7Lf3ymZXl1Bnba9sfSpnkqolJng