試験の準備方法-ユニークなSC-200勉強資料試験-効率的なSC-200独学書籍

P.S.Xhs1991がGoogle Driveで共有している無料の2026 Microsoft SC-200ダンプ：https://drive.google.com/open?id=1uSpZjkshXfv4Hnp4G4LPAkSguo-tH9QD

MicrosoftのSC-200認定試験を受験する気があるのですか。この試験を受けた身の回りの人がきっと多くいるでしょう。これは非常に大切な試験で、試験に合格してSC-200認証資格を取ると、あなたは多くのメリットを得られますから。では、他の人を頼んで試験に合格する対策を教えてもらったのですか。試験に準備する方法が色々ありますが、最も高効率なのは、きっと良いツールを利用することですね。ところで、あなたにとってどんなツールが良いと言えるのですか。もちろんXhs1991のSC-200問題集です。

Microsoft SC-200 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• セキュリティ運用環境の管理: この試験のトピックでは、Microsoft Defender XDR での設定の構成方法、資産と環境の管理、Microsoft Sentinel ワークスペースの設計と構成、Microsoft Sentinel でのデータ ソースの取り込みについて説明します。
トピック 2	• インシデント対応の管理: このセクションでは、Microsoft Defender XDR でのアラートとインシデントへの対応について説明します。また、Microsoft Defender for Endpoint によって特定されたアラートとインシデントへの対応、および Microsoft Sentinel でのセキュリティ オーケストレーション、自動化、および対応 (SOAR) の構成についても説明します。
トピック 3	• 保護と検出を構成する: このセクションでは、Microsoft Defender セキュリティ テクノロジでの保護の構成、Microsoft Defender XDR での検出の構成、および Microsoft Sentinel での検出の構成について説明します。
トピック 4	• 脅威ハンティングの実行: 試験のこのセクションでは、KQL と Microsoft Sentinel を使用して脅威をハンティングする方法について説明します。また、ワークブックを使用してデータを分析および解釈することも含まれます。

>> SC-200勉強資料 <<

効果的-ハイパスレートのSC-200勉強資料試験-試験の準備方法SC-200独学書籍

SC-200試験の急流を学び、SC-200試験を準備するのに20〜30時間しかかかりません。多くの人々、特に現職のスタッフは仕事、学習、家族生活、その他の重要な事柄で忙しく、SC-200試験を学習して準備する時間とエネルギーがほとんどありません。しかし、SC-200テストトレントを購入すれば、最も重要なことにメインエネル

ギーを投資し、試験を学習して準備するために毎日1〜2時間を割くことができます。 SC-200試験の質問と回答は実際の試験に基づいており、Microsoft Security Operations Analyst受験者の一般的な傾向に準拠しています。

Microsoft SC-200認定試験は、セキュリティの基礎、脅威インテリジェンス、セキュリティ運用、インシデント対応、ガバナンス、リスク、コンプライアンス（GRC）など、幅広いトピックをカバーしています。また、実際のセキュリティインシデントをシミュレートし、セキュリティの脅威を特定、調査、および対応するために知識とスキルを適用する必要がある実用的なシナリオも含まれています。試験形式は複数選択であり、完了するには180分かかります。

Microsoft Security Operations Analyst 認定 SC-200 試験問題 (Q233-Q238):

質問 # 233
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.

正解：

解説：
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

質問 # 234
You have a custom detection rule that includes the following KQL query.
For each of the following statements, select Yes if True. Otherwise select No.
NOTE: Each correct selection is worth one point.

正解：

解説：

質問 # 235
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.

正解：

解説：
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

質問 # 236
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.

正解：

解説：
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

質問 # 237
You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

- A. Configure the Diagnostics settings in Azure AD to stream to an event hub.
- B. Create an Azure Sentinel workspace that has an Azure Active Directory connector.
- C. Create an Azure Sentinel workspace that has a Security Events connector.
- D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

正解：A

解説：
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring
Topic 1, Contoso Ltd
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
A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.
Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.
Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements

Contoso identifies the following technical requirements:
Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True

質問 # 238
.....