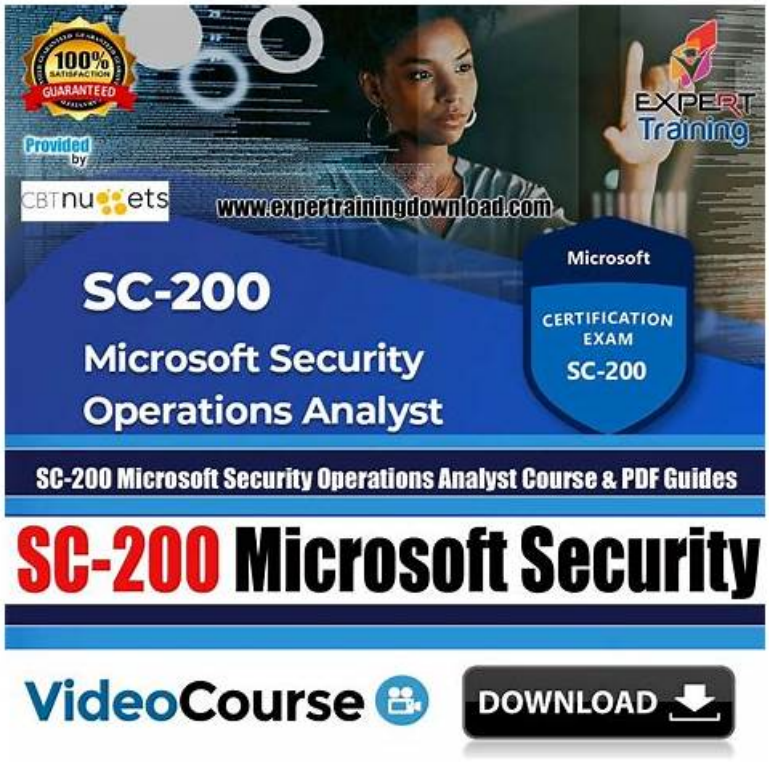
Free PDF Quiz 2026 Microsoft Fantastic SC-200: Microsoft Security Operations Analyst Latest Test Prep



P.S. Free & New SC-200 dumps are available on Google Drive shared by PracticeVCE: https://drive.google.com/open?id=1TZBQNQT8u_fopIlHVI3f-IZfSSOmhdFO

Our excellent Microsoft SC-200 practice materials beckon exam candidates around the world with their attractive characters. Our experts made significant contribution to their excellence. So we can say bluntly that our SC-200 Actual Exam is the best. Our effort in building the content of our SC-200 study dumps lead to the development of SC-200 learning guide and strengthen their perfection.

Microsoft SC-200 (Microsoft Security Operations Analyst) Exam is a valuable certification for professionals looking to advance their career in security operations. It provides a comprehensive coverage of the skills and knowledge required to perform security operations tasks and demonstrates the candidate's proficiency in Microsoft security technologies. By achieving this certification, professionals can enhance their credentials and demonstrate their commitment to the field of security operations.

>> SC-200 Latest Test Prep <<

Dumps SC-200 Free - SC-200 Reliable Braindumps Ppt

If you have been very panic sitting in the examination room, our SC-200 actual exam allows you to pass the exam more calmly and calmly. After you use our products, our SC-200 study materials will provide you with a real test environment before the SC-200 Exam. After the simulation, you will have a clearer understanding of the exam environment, examination process, and exam outline. And our SC-200 learning guide will be your best choice.

Microsoft SC-200 exam, also known as the Microsoft Security Operations Analyst exam, is a highly sought-after certification for professionals working in the field of cybersecurity. SC-200 Exam is designed to test the candidate's knowledge and skills in threat detection, incident response, and compliance management.

Microsoft Security Operations Analyst Sample Questions (Q458-Q463):

NEW QUESTION # 458

You have a Microsoft Sentinel workspace named SW1.
You need to identify which anomaly rules are enabled in SW1.
What should you review in Microsoft Sentinel?

- A. Analytics
- B. Entity behavior
- C. Settings
- D. Content hub

Answer: A

NEW QUESTION # 459
Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.
You need to identify which Office VBA macros might be affected.
Which two commands can you run to achieve the goal?Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A.
- B.
- C.
- D.

Answer: A,D

Explanation:
Must use Set-MpPreference with Enabled and then Add-MpPreference with Enabled. Audit does not block.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface- reduction?view=o365-worldwide#powershell

NEW QUESTION # 460
You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1.
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for WS1. The solution must follow the principle of least privilege.
Which roles should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:

NEW QUESTION # 461
You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.
You are notified that the account of User1 is compromised.
You need to review the alerts triggered on the devices to which User1 signed in.
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:
Explanation:
Box 1: join
An inner join.
This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.

This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.
DeviceInfo
//Query for devices that the potentially compromised account has logged onto
| where LoggedOnUsers contains '<account-name>'
| distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
| join kind=inner AlertEvidence on DeviceId
| project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"
Box 2: project
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails- devices?view=o365-worldwide

NEW QUESTION # 462
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint and contains a user named user1 and a Microsoft 365 group named Group1. All users are assigned a Defender for Endpoint Plan 1 license.
You enable Microsoft Defender XDR Unified role-based access control (RBAC) for Endpoints & Vulnerability Management.
You need to ensure that User1 can configure alerts that will send email notifications to Group1. The solution must follow the principle of least privilege.
Which permissions should you assign to User1?

- A. Defender Vulnerability Management - Remediation handling
- B. Manage security settings
- C. Alerts investigation
- D. Live response capabilities: Basic

Answer: B

Explanation:
You have a Microsoft 365 subscription with Defender for Endpoint, and you've enabled Microsoft Defender XDR unified RBAC for Endpoints & Vulnerability Management. The requirement is that User1 should be able to configure alerts (i.e. set up rules that send email notifications) such that emails go to Group1, and you want to follow least privilege-that is, grant the minimal permission necessary for that capability.
Microsoft's official documentation states:
"Only users with 'Manage security settings' permissions can configure email notifications." Microsoft Learn Thus, in the Defender XDR RBAC model, the permission that allows a user to create or modify email notification alert rules is tied to Manage security settings (also referred to as core security settings in some documentation) .
Furthermore, the "Alert policies in the Microsoft Defender portal" article indicates that to create or edit alert policies (i.e. rules that govern how alerts behave and who they notify), you need the Manage Alerts role or equivalent permissions. However, in the unified RBAC model, managing alert policies overlaps with the broader "security settings" capability. Microsoft Learn Therefore:
* Granting Manage security settings gives exactly the ability required to configure email notification rules for alerts (including targeting the Microsoft 365 group) without giving broader investigative or remediation privileges.
* Other permissions-e.g., "Alerts investigation" (allows investigating alerts), "Defender Vulnerability Management - Remediation handling" (for handling remediation tasks), or "Live response capabilities:
Basic" (for remote response actions)-do not cover alert notification configuration.
Hence the correct, least-privilege RBAC permission to assign to User1 is Manage security settings.

NEW QUESTION # 463
.....

➥ www.pdfvce.com □ and search for ➽ SC-200 □ to download exam materials for free □SC-200 Trustworthy Exam Torrent

- Quiz Latest Microsoft - SC-200 Latest Test Prep □ Copy URL ✔ www.pdfdumps.com □✔□ open and search for □ SC-200 □ to download for free □Pass SC-200 Exam
- SC-200 Guaranteed Passing □ Latest SC-200 Dumps Questions □ SC-200 Online Lab Simulation □ ➥ www.pdfvce.com □ is best website to obtain ☀ SC-200 □☀□ for free download □New SC-200 Test Price
- 2026 SC-200 Latest Test Prep | High-quality Microsoft Dumps SC-200 Free: Microsoft Security Operations Analyst □ Copy URL { www.practicevce.com } open and search for ☀ SC-200 □☀□ to download for free □SC-200 Latest Test Pdf
- Quiz Latest Microsoft - SC-200 Latest Test Prep □ Search for □ SC-200 □ and obtain a free download on { www.pdfvce.com } □Valid SC-200 Exam Questions
- ThreeFormats of www.vce4dumps.com Microsoft SC-200 Practice Test Questions □ Search for [SC-200] on □ www.vce4dumps.com □ immediately to obtain a free download □New SC-200 Test Price
- Updated SC-200 Latest Test Prep for Real Exam □ Search for □ SC-200 □ and download it for free on 《 www.pdfvce.com 》 website □New SC-200 Dumps Book
- SC-200 Valid Dumps Free □ SC-200 Valid Braindumps Sheet □ Exam SC-200 Questions ❤□ Simply search for ☀ SC-200 □☀□ for free download on ▹ www.pass4test.com ◃ □Test SC-200 Dates
- New SC-200 Test Price □ Exam SC-200 Questions □ SC-200 Valid Dumps Free □ The page for free download of □ SC-200 □ on [www.pdfvce.com] will open immediately □Reliable SC-200 Test Cost
- SC-200 Exam Brain Dumps □ Valid SC-200 Exam Questions □ Pass SC-200 Exam □ Search for ➽ SC-200 □ and download it for free on ➤ www.pdfdumps.com □ website □New SC-200 Dumps Book
- sairaplft208767.blogsumer.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, roydeto812541.wikijm.com, saulwzfv601211.lotrlegendswiki.com, emilytrwm749957.blogdemls.com, anyacqsf262601.ourabilitywiki.com, esmeercoi551394.techionblog.com, saadbrra364066.snack-blog.com, robertwanj963022.therainblog.com, Disposable vapes

2026 Latest PracticeVCE SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1TZBQNQT8u_fopIlHVI3f-IZfSSOmhdFO