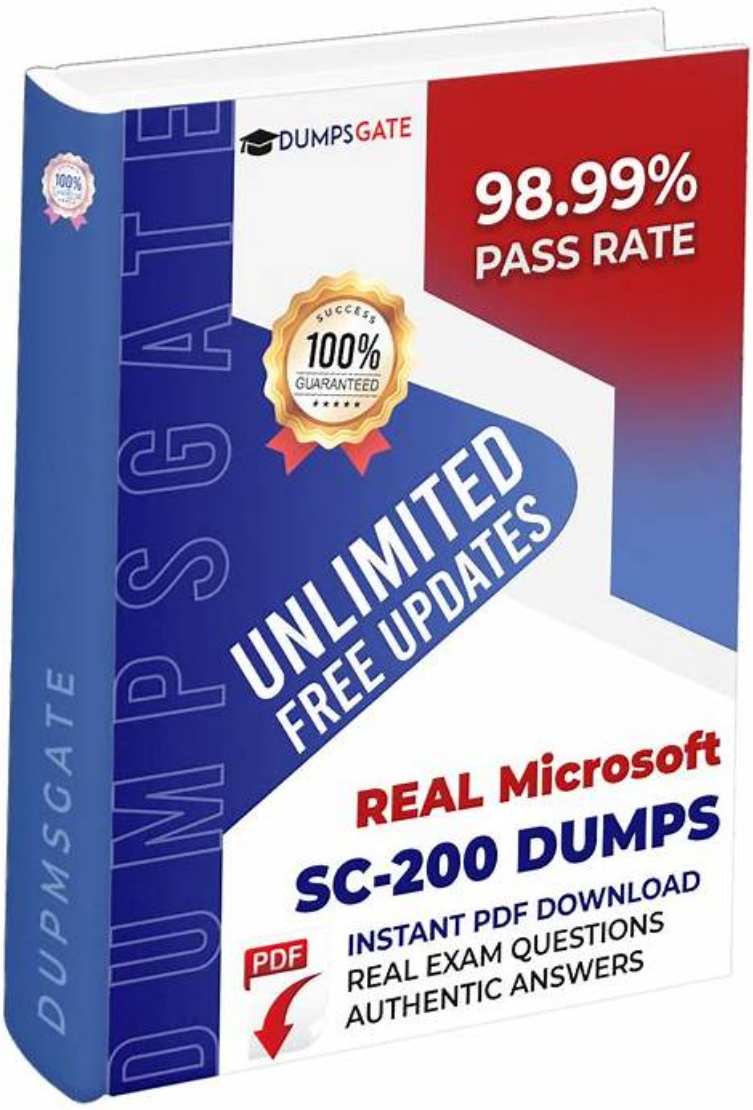
Microsoft SC-200 Exam Dumps - Easiest Preparation Method [2026]



P.S. Free & New SC-200 dumps are available on Google Drive shared by ValidBraindumps: https://drive.google.com/open?id=1cSu5GYi1oGKNiZR51_9WhnNS4Dq_5Blt

We all know the effective diligence is in direct proportion to outcome, so by years of diligent work, our experts have collected the frequent-tested knowledge into our Microsoft SC-200 practice materials for your reference. So our Microsoft Security Operations Analyst training materials are triumph of their endeavor.

Microsoft SC-200 exam is designed for security professionals who are responsible for protecting the organization's infrastructure from cyber threats. SC-200 exam covers a wide range of topics, including threat management, identity and access management, cloud security, compliance, and governance. SC-200 Exam also covers the use of Microsoft's security products, such as Azure Security Center, Microsoft 365 Defender, and Microsoft Defender for Endpoint.

>> SC-200 New Braindumps Ebook <<

New SC-200 New Braindumps Ebook Free PDF | Efficient SC-200 Certification Training: Microsoft Security Operations Analyst

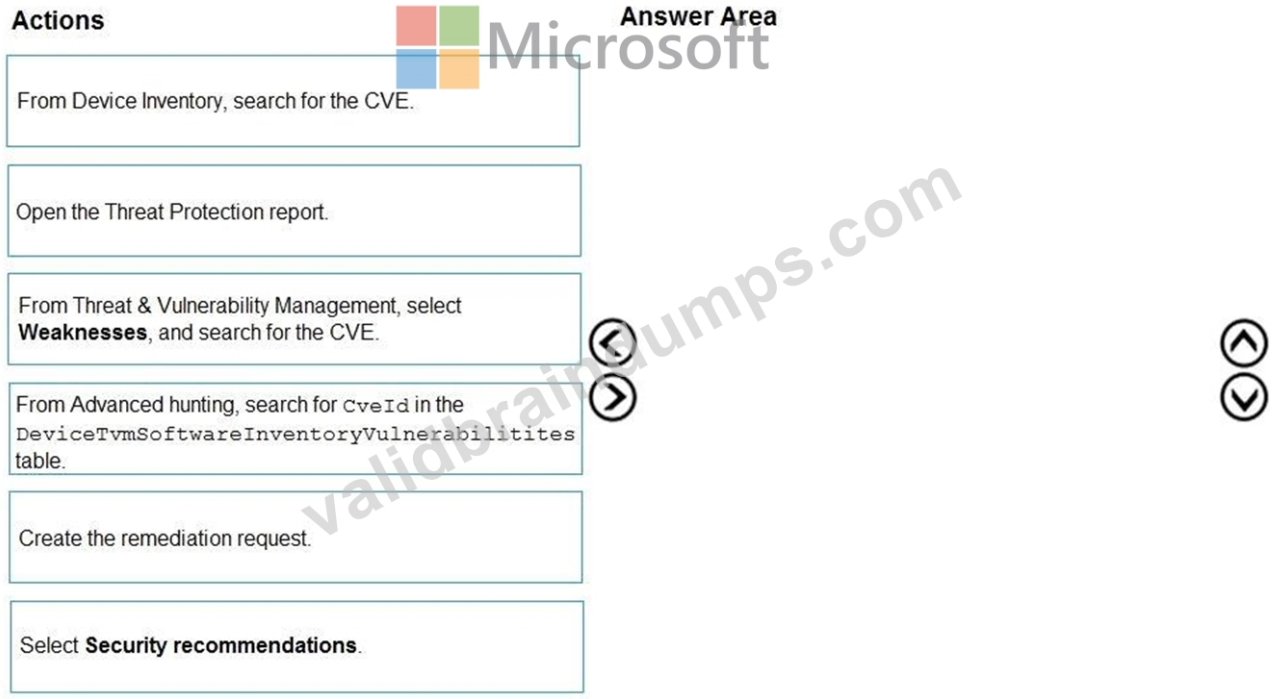
It is believe that employers nowadays are more open to learn new knowledge, as they realize that Microsoft certification may be conducive to them in refreshing their life, especially in their career arena. A professional Microsoft certification serves as the most powerful way for you to show your professional knowledge and skills. For those who are struggling for promotion or better job, they should figure out what kind of SC-200 Test Guide is most suitable for them. However, some employers are hesitating to choose. With our high-accuracy SC-200 test guide, our candidates can grasp the key points, and become sophisticated with the exam content. You only need to spend 20-30 hours practicing with our Microsoft Security Operations Analyst learn tool, passing the exam would be a piece of cake.

Certification Topics of Microsoft SC-200 Exam

- Mitigate threats using Azure Sentinel (40-45%)
- Mitigate threats using Microsoft 365 Defender (25-30%)
- Mitigate threats using Azure Defender (25-30%)

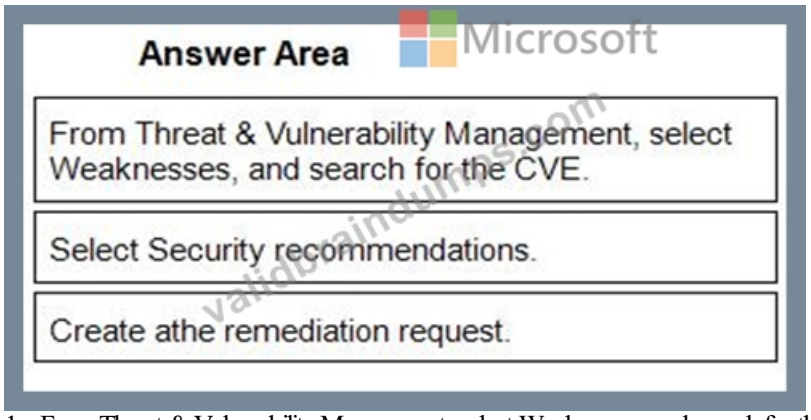
Microsoft Security Operations Analyst Sample Questions (Q92-Q97):

NEW QUESTION # 92
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
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.



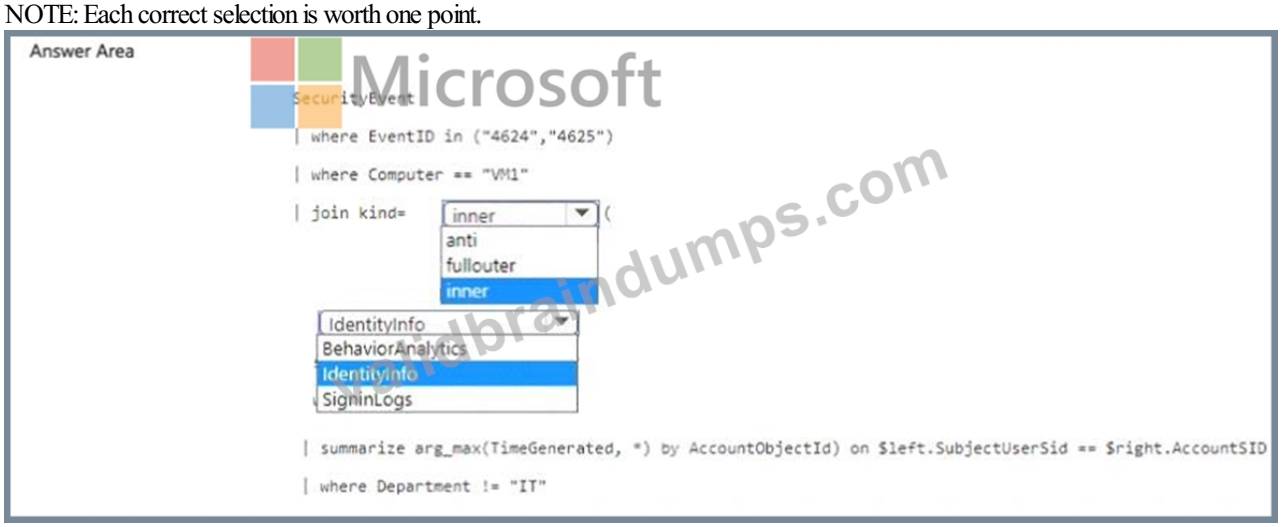
Answer:

Explanation:



1 - From Threat & Vulnerability Management, select Weaknesses, and search for the CVE.
2 - Select Security recommendations.
3 - Create athe remediation request.
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

NEW QUESTION # 93
You have an Azure subscription that contains the following resources:
* A virtual machine named VM1 that runs Windows Server
* A Microsoft Sentinel workspace named Sentinel1 that has User and Entity Behavior Analytics (UEBA) enabled You have a scheduled query rule named Rule1 that tracks sign-in attempts to VM1.
You need to update Rule 1 to detect when a user from outside the IT department of your company signs in to VM1. The solution must meet the following requirements:
* Utilize UEBA results.
* Maximize query performance.
* Minimize the number of false positives.
How should you complete the rule definition? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:
Explanation:

NEW QUESTION # 94
You have the following environment:
* Azure Sentinel
* A Microsoft 365 subscription
* Microsoft Defender for Identity

* An Azure Active Directory (Azure AD) tenant
You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Configure auditing in the Microsoft 365 compliance center.
- B. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
- C. Configure Windows Event Forwarding on the domain controllers.
- D. Modify the permissions of the Domain Controllers organizational unit (OU).

Answer: B,C

Explanation:
Microsoft Defender for Identity (MDI) detects sensitive group modifications-such as changes to Domain Admins, Enterprise Admins, or Schema Admins-by analyzing Windows security events from domain controllers. For MDI sensors to detect such changes, advanced audit policies must be configured to log these activities (specifically Directory Service Changes and Account Management events).
Microsoft documentation specifies that "Defender for Identity requires auditing to be enabled on domain controllers for security events like group membership changes." This is done under Advanced Audit Policy Configuration # Directory Service Changes.
Additionally, Windows Event Forwarding (WEF) is required or beneficial when Azure Sentinel needs to centralize those events from multiple domain controllers into a Log Analytics workspace. WEF minimizes administrative effort by automatically collecting logs without manual export or per-server log pulling.
Thus, configuring Advanced Audit Policy ensures the right events are generated, and Windows Event Forwarding ensures those events reach Sentinel for correlation with MDI alerts.
Correct Answers: A and D

NEW QUESTION # 95
You have the following SQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```


Answer:

Explanation:
Explanation:

NEW QUESTION # 96
You have an Azure subscription that contains 100 Linux virtual machines.
You need to configure Microsoft Sentinel to collect event logs from the virtual machines.
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.

Answer:

Explanation:
Explanation

NEW QUESTION # 97

.....

SC-200 Certification Training: https://www.validbraindumps.com/SC-200-exam-prep.html

- Exam SC-200 Tests □ SC-200 Sample Questions □ Latest Braindumps SC-200 Ppt □ Simply search for { SC-200 } for free download on ▸ www.prepawaypdf.com ◂ □Latest Braindumps SC-200 Ppt
- Sample SC-200 Questions □ Latest Braindumps SC-200 Ppt □ Test SC-200 Price □ Search for ▸ SC-200 ◂ and download it for free immediately on ▹ www.pdfvce.com ◃ □SC-200 Valid Study Plan
- SC-200 Exam Guide □ Sample SC-200 Questions □ Relevant SC-200 Questions □ Download 「 SC-200 」 for free by simply searching on ➡ www.practicevce.com □□□ □Training SC-200 Materials
- SC-200 Valid Study Plan □ SC-200 Latest Demo □ Training SC-200 Materials □ Go to website ☀ www.pdfvce.com □☀□ open and search for （ SC-200 ） to download for free □SC-200 Exam Guide
- Test SC-200 Price □ Reliable SC-200 Test Practice ✍ SC-200 New Real Test □ Search for ☀ SC-200 □☀□ and download it for free immediately on □ www.practicevce.com □ □Training SC-200 Materials
- SC-200 Sample Questions □ Certification SC-200 Dumps □ Customized SC-200 Lab Simulation □ Immediately open ✔ www.pdfvce.com □✔□ and search for □ SC-200 □ to obtain a free download □SC-200 Latest Demo
- Get Special 25% EXTRA Discount on SC-200 Dumps By www.troytecdumps.com □ Open website ➤ www.troytecdumps.com □ and search for ➥ SC-200 □ for free download □SC-200 Exam Cram
- 100% Pass Quiz Updated SC-200 - Microsoft Security Operations Analyst New Braindumps Ebook □ Download [SC-200] for free by simply entering ➠ www.pdfvce.com □ website □Customized SC-200 Lab Simulation
- SC-200 Sample Questions □ SC-200 Reliable Test Experience □ Exam SC-200 Tests □ Enter 「 www.prepawayete.com 」 and search for ✔ SC-200 □✔□ to download for free □Training SC-200 Materials
- Easy to Use Pdfvce Microsoft SC-200 Practice Questions Formats □ Search for □ SC-200 □ and download it for free on ⇛ www.pdfvce.com ⇚ website □Exam SC-200 Overviews
- Get Special 25% EXTRA Discount on SC-200 Dumps By www.vceengine.com □ " www.vceengine.com " is best website to obtain ➠ SC-200 □ for free download □SC-200 Certification Torrent
- 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, 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, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.askmap.net, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest ValidBraindumps SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1cSu5GYi1oGKNiZR51_9WhnNS4Dq_5Blt