# 2025 Unparalleled Microsoft SC-200 Exam Brain Dumps Pass Guaranteed Quiz


BTW, DOWNLOAD part of ExamPrepAway SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=1e_Cnow3b0RVu2oBxcyP7wXLy_AvLCjqO

For example, if you are a college student, you can learn and use online resources through the student learning platform over the SC-200 study materials. On the other hand, the SC-200 study engine are for an office worker, free profession personnel have different learning arrangement, such extensive audience greatly improved the core competitiveness of our SC-200 Exam Questions, to provide users with better suited to their specific circumstances of high quality learning resources, according to their aptitude, on-demand, maximum play to the role of the SC-200 exam questions.

Microsoft SC-200 certification exam is an excellent way for security professionals to demonstrate their expertise in security operations. Microsoft Security Operations Analyst certification exam is based on the latest security operations best practices and methodologies, and it is designed to validate your skills in a variety of areas, including incident response, threat intelligence, and security controls. By passing the exam, you will demonstrate your ability to identify and mitigate security threats, analyze security data, and respond to security incidents.

Microsoft SC-200 (Microsoft Security Operations Analyst) Exam is a certification exam offered by Microsoft that validates the skills and knowledge of security operations professionals. SC-200 exam is designed for individuals who have experience in analyzing security data, detecting threats, and responding to security incidents. Microsoft Security Operations Analyst certification covers various topics such as threat intelligence, security operations center (SOC) operations, incident response, and compliance.

**>> SC-200 Exam Brain Dumps <<**

## New Microsoft SC-200 Exam Camp | New SC-200 Test Topics

If you are wandering for SC-200 study material and the reliable platform that will lead you to success in exam, then stop considering this issue. ExamPrepAway is the solution to your problem. They offer you reliable and updated SC-200 exam questions. The exam questions are duly designed by the team of subject matter experts; they are highly experienced and trained in developing exam material. ExamPrepAway offers a 100% money back guarantee, in case you fail in your SC-200. You claim revert, by showing your transcript and undergoing through the clearance process. Also, we provide 24/7 customer service to all our valued customers. Our dedicated team will answer all your all queries related to SC-200.

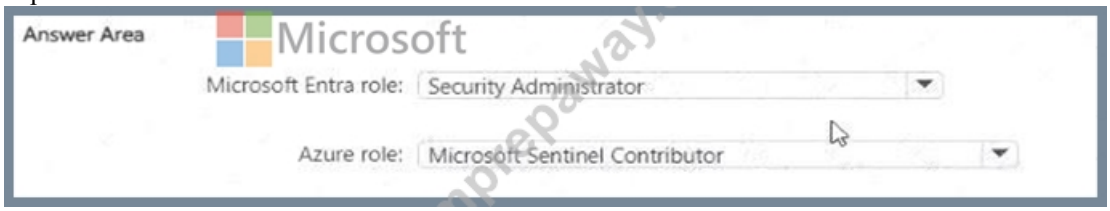
## Microsoft Security Operations Analyst Sample Questions (Q286-Q291):

**NEW QUESTION # 286**
You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in the Microsoft Entra tenant. The solution must use 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:

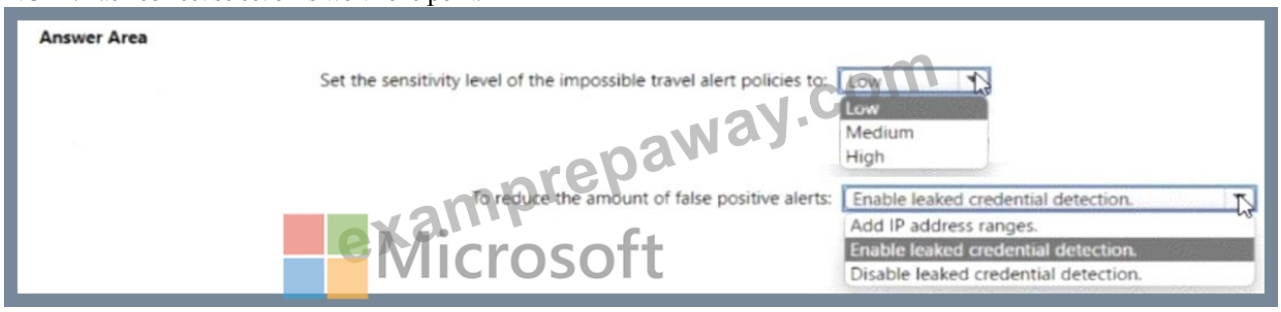

Explanation:




Enabling User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel requires specific permissions in both Microsoft Entra ID (Azure AD) and the Azure Sentinel workspace. The goal is to grant the least privilege necessary for the user (User1) to enable UEBA and manage entity behavior analytics.
Microsoft's documentation for UEBA setup specifies that to enable UEBA for an Entra tenant, the user must have access to identity-related signals and security settings within the Microsoft Entra environment.
Specifically:
"To enable UEBA and connect Microsoft Entra ID data, the user must be assigned the Security Administrator role in Microsoft Entra ID. This role allows management of security-related features without granting full directory or global admin privileges." The Security Administrator role provides just enough access to security configurations, alerts, and risk data, aligning with the principle of least privilege.
Other roles:
* Global Administrator is overly privileged.
* Security Operator can only view alerts, not configure settings.
* Identity Governance Administrator focuses on access reviews and entitlement management, not UEBA setup.
Hence, the correct Entra role is Security Administrator.
For the Azure side, Microsoft's official Sentinel RBAC guidance states:
"To enable or configure UEBA in a Sentinel workspace, the user must have the Microsoft Sentinel Contributor role. This role allows

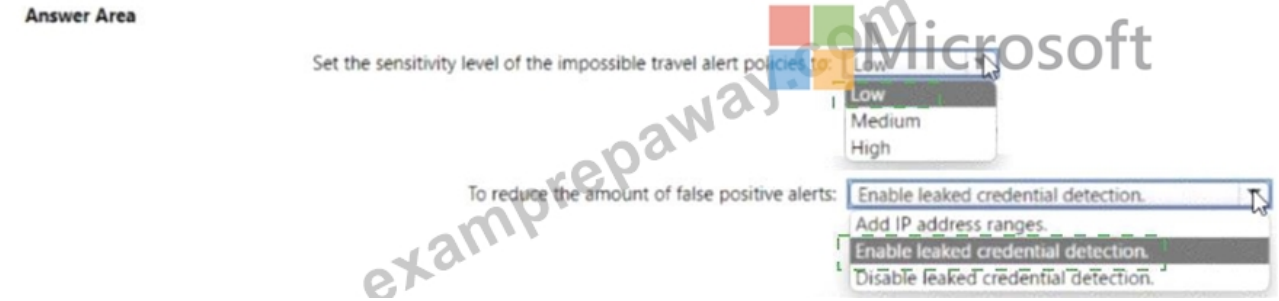
enabling and configuring UEBA, managing analytics, and viewing data within Sentinel." The Sentinel Contributor role grants permissions to configure data connectors, UEBA settings, and entity analytics features but not workspace-wide administrative rights.
Other options:
* Microsoft Sentinel Automation Contributor is limited to playbook and automation configurations.
* Security Admin and Security Assessment Contributor roles apply to Microsoft Defender for Cloud and general Azure security posture, not UEBA configuration.
# Final Correct Roles:
* Microsoft Entra role: Security Administrator
* Azure role: Microsoft Sentinel Contributor

**NEW QUESTION # 287**
You need to meet the Microsoft Defender for Cloud Apps requirements
What should you do? To answer. select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

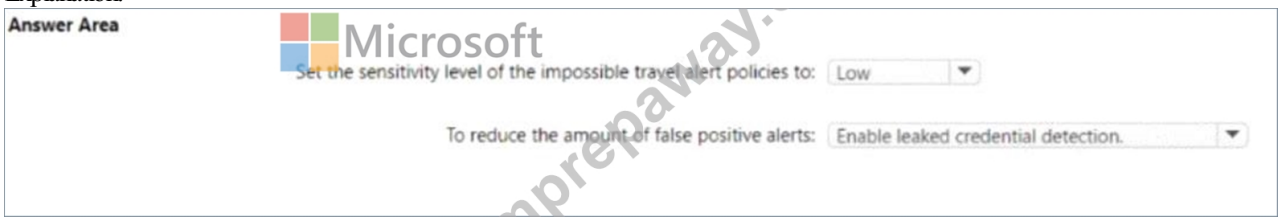



**Answer:**

Explanation:




Explanation:

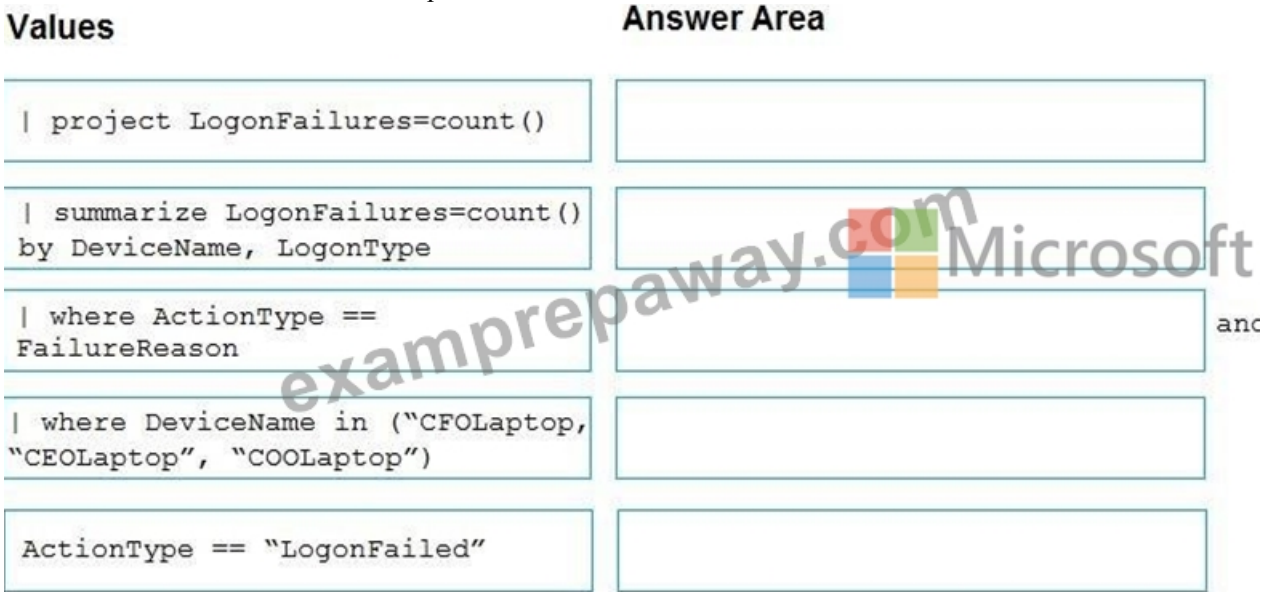



**NEW QUESTION # 288**
You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schem a. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

- A. Copy the parsers to the Azure Monitor Logs page.
- B. Create a YAML file based on the DNS template.
- C. Create an XML file based on the DNS template.
- D. Create a JSON file based on the DNS template.

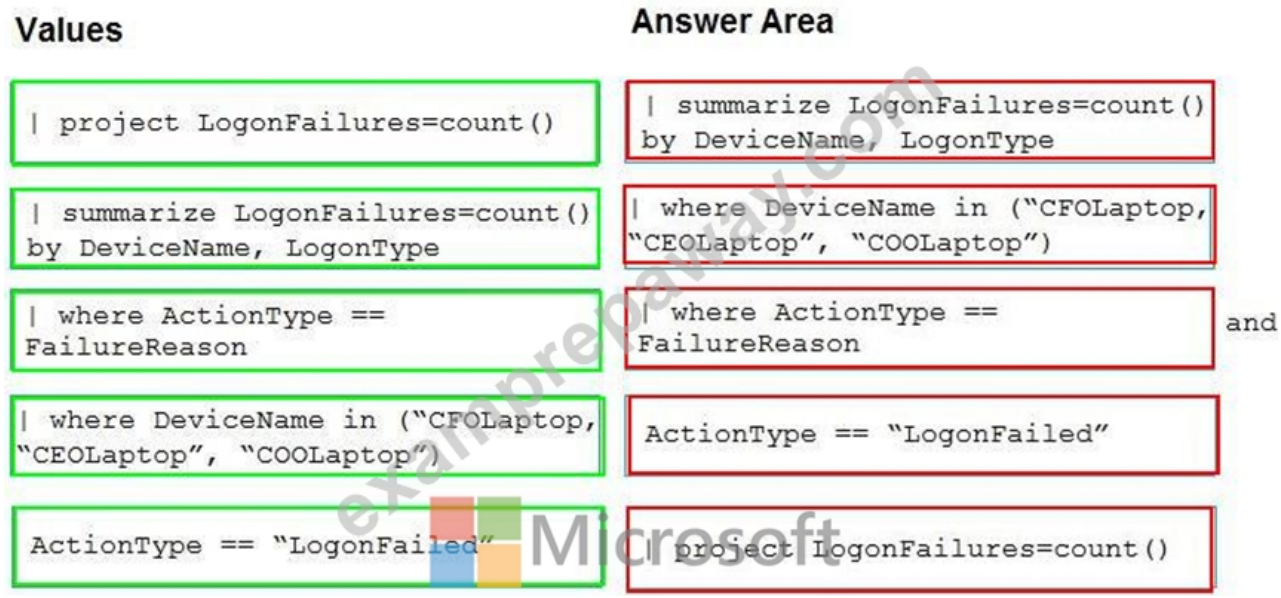
**Answer: A**

**NEW QUESTION # 289**
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

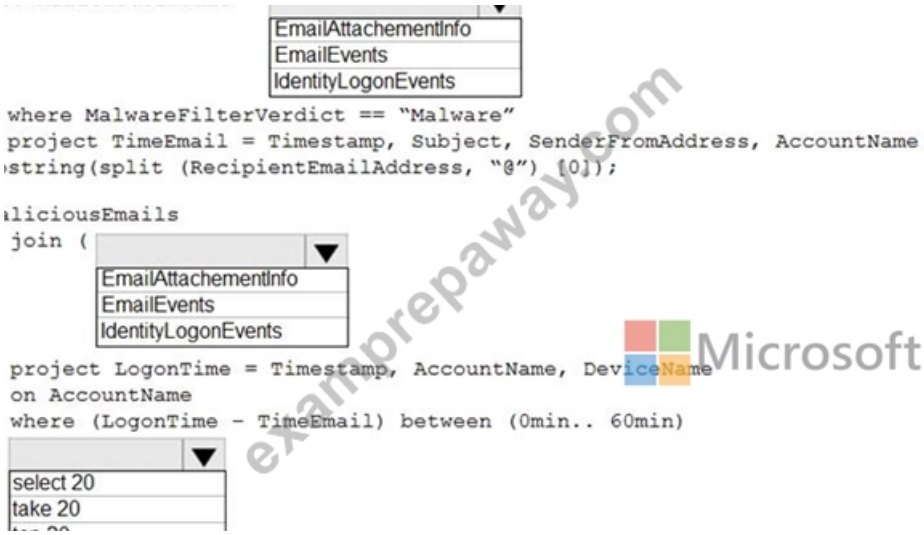



**Answer:**

Explanation:

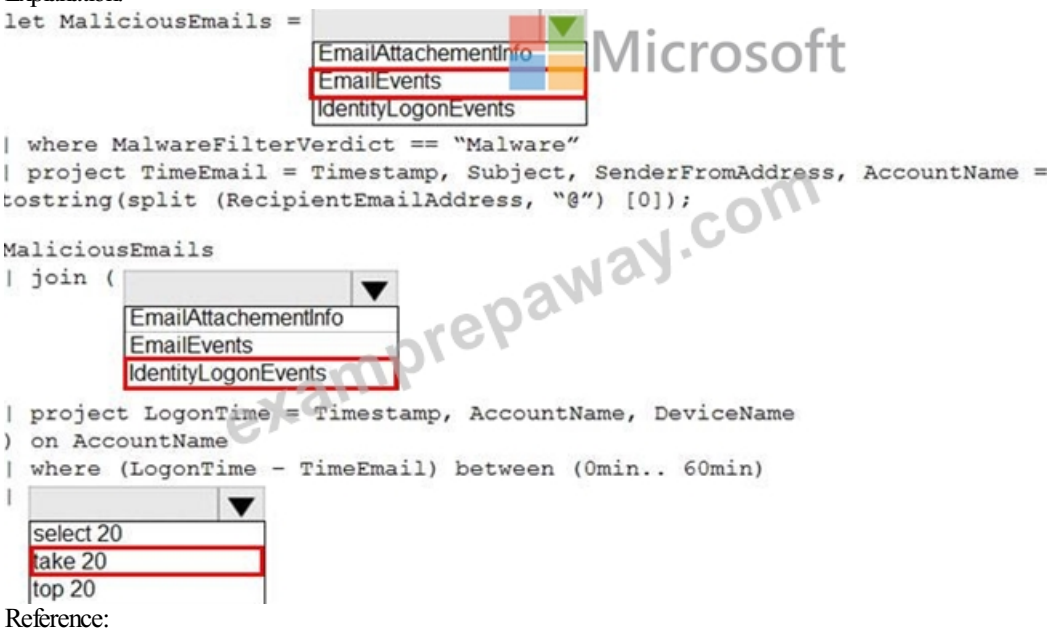



**NEW QUESTION # 290**
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
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:




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

**NEW QUESTION # 291**
.....

In recruiting employees as IT engineers many companies look for evidence of all-round ability especially constantly studying ability more their education background. SC-200 dumps torrent can help you fight for Microsoft certification and achieve your dream in the shortest time. If you want to stand out from the crowd, purchasing a valid SC-200 Dumps Torrent will be a shortcut to success. It will be useful for you to avoid detours and save your money & time.

immediately □Valid SC-200 Braindumps

- SC-200 Exam Brain Dumps 100% Pass | Valid New SC-200 Exam Camp: Microsoft Security Operations Analyst □ Copy URL □ www.passtestking.com □ open and search for ▸ SC-200 ◂ to download for free □SC-200 Exam Objectives
- Quiz 2025 SC-200: Microsoft Security Operations Analyst Latest Exam Brain Dumps □ Open website □ www.pdfvce.com □ and search for 「 SC-200 」 for free download □Flexible SC-200 Learning Mode
- Microsoft Security Operations Analyst Exam Lab Questions - SC-200 valid VCE test - Microsoft Security Operations Analyst Exam Simulator Online □ Easily obtain free download of [ SC-200 ] by searching on ➤ www.exam4pdf.com □ □ □Dumps SC-200 Discount
- Pass SC-200 Test □ SC-200 Reliable Test Preparation □ Test SC-200 Assessment □ Open ➥ www.pdfvce.com □ □ enter ▸ SC-200 ◂ and obtain a free download □SC-200 Latest Exam Papers
- Valid SC-200 Braindumps □ Valid SC-200 Braindumps □ New SC-200 Exam Papers □ Search for ➠ SC-200 □ and download it for free on ➤ www.exams4collection.com □ website □Flexible SC-200 Learning Mode
- New SC-200 Exam Brain Dumps | High-quality Microsoft New SC-200 Exam Camp: Microsoft Security Operations Analyst □ Search for ⇛ SC-200 ⇚ and download it for free on ➠ www.pdfvce.com □ website □SC-200 Reliable Test Preparation
- SC-200 Valid Dumps Demo □ SC-200 Valid Exam Question □ Pass SC-200 Test □ Open ➤ www.prep4away.com □ and search for 《 SC-200 》 to download exam materials for free □SC-200 Valid Dumps Ebook
- 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, mdiaustralia.com, unldigiwithweb.online, wzsj.lwtcc.cn, fordimir.net, 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, kareyed271.idblogz.com, daotao.wisebusiness.edu.vn, 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

BTW, DOWNLOAD part of ExamPrepAway SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=1e_Cnow3b0RVu2oBxcyP7wXLy_AvLCjqO