Quiz SC-200 - Fantastic Free Microsoft Security Operations Analyst Practice

2025 Latest Exam4Tests SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1GcSicQUd7sIpCuRB3B0Be05292-9R-t5

Our company has built the culture of integrity from our establishment. You just need to pay the relevant money for the SC-200 practice materials. Our system will never deduct extra money from your debit cards. Also, your payment information of the SC-200 Study Materials will be secret. No one will crack your passwords. Our payment system will automatically delete your payment information once you finish paying money for our SC-200 exam questions.

Microsoft SC-200 Exam measures the skills and knowledge needed to perform security operations tasks such as identifying and investigating security incidents, configuring security solutions, and implementing security controls. Microsoft Security Operations Analyst certification exam is designed to validate the skills of security professionals who are responsible for protecting Microsoft environments against cyber threats. The SC-200 exam is an important step towards obtaining other Microsoft security certifications, such as the Microsoft Certified: Azure Security Engineer Associate certification.

Microsoft Security Operations Analyst certification exam, also known as SC-200, is designed for security professionals who are responsible for managing and monitoring security solutions in an organization. Microsoft Security Operations Analyst certification validates the skills and knowledge required to protect an organization's assets, detect and respond to security threats, and manage security operations.

Achieving the Microsoft Security Operations Analyst certification can be a valuable asset for security professionals looking to advance their careers in the field of cybersecurity. Microsoft Security Operations Analyst certification demonstrates that the candidate has the skills and knowledge necessary to detect, investigate, and respond to security incidents in a Microsoft environment and can be a valuable addition to any security team.

>> Free SC-200 Practice <<

Customizable SC-200 Exam Mode | Reliable SC-200 Practice Questions

Almost those who work in the IT industry know that it is very difficult to prepare for SC-200. Although our Exam4Tests cannot reduce the difficulty of SC-200 exam, what we can do is to help you reduce the difficulty of the exam preparation. Once you have tried our technical team carefully prepared for you after the test, you will not fear to SC-200 Exam. What we have done is to make you more confident in SC-200 exam.

Microsoft Security Operations Analyst Sample Questions (Q270-Q275):

NEW QUESTION # 270
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
* Microsoft Excel macros that download scripts from untrusted websites
* Users that open executable attachments in Microsoft Outlook
* Outlook rules and forms exploits
What should you use?

- A. attack surface reduction rules in Microsoft Defender for Endpoint
- B. Microsoft Defender Antivirus
- C. adaptive application control in Azure Defender
- D. Windows Defender Firewall

Answer: A

Explanation:
According to official Microsoft Defender for Endpoint documentation, Attack Surface Reduction (ASR) rules are specifically designed to block behaviors commonly used by malware and ransomware, such as malicious macro execution, script downloads from untrusted sources, and the abuse of Office applications to launch harmful executables or exploits.
In this scenario:
* Excel macros downloading scripts from untrusted websites are mitigated by the ASR rule:"Block Office applications from creating child processes" and "Block Office communication application from creating child processes."
* Users opening executable attachments in Outlook are covered by:"Block executable content from email and webmail."
* Outlook rules and forms exploits are addressed by:"Block Office applications from injecting code into other processes."
Microsoft's Defender for Endpoint security baseline and documentation highlight that these rules "reduce the attack surface by minimizing the number of entry points an attacker can use to exploit a system." Administrators can configure them through Microsoft Intune, Group Policy, or PowerShell, and monitor their effectiveness in the Microsoft 365 Defender portal under Threat & Vulnerability Management.
Other options like Defender Antivirus (A) focus on detecting known malware after execution rather than blocking risky behaviors preemptively. Windows Defender Firewall (C) controls network traffic, not application-level threats. Adaptive application control in Azure Defender (D) is used for whitelisting applications on Azure VMs, not on Microsoft 365 endpoints.
Therefore, the correct answer is:
B: Attack surface reduction rules in Microsoft Defender for Endpoint
o365-worldwide

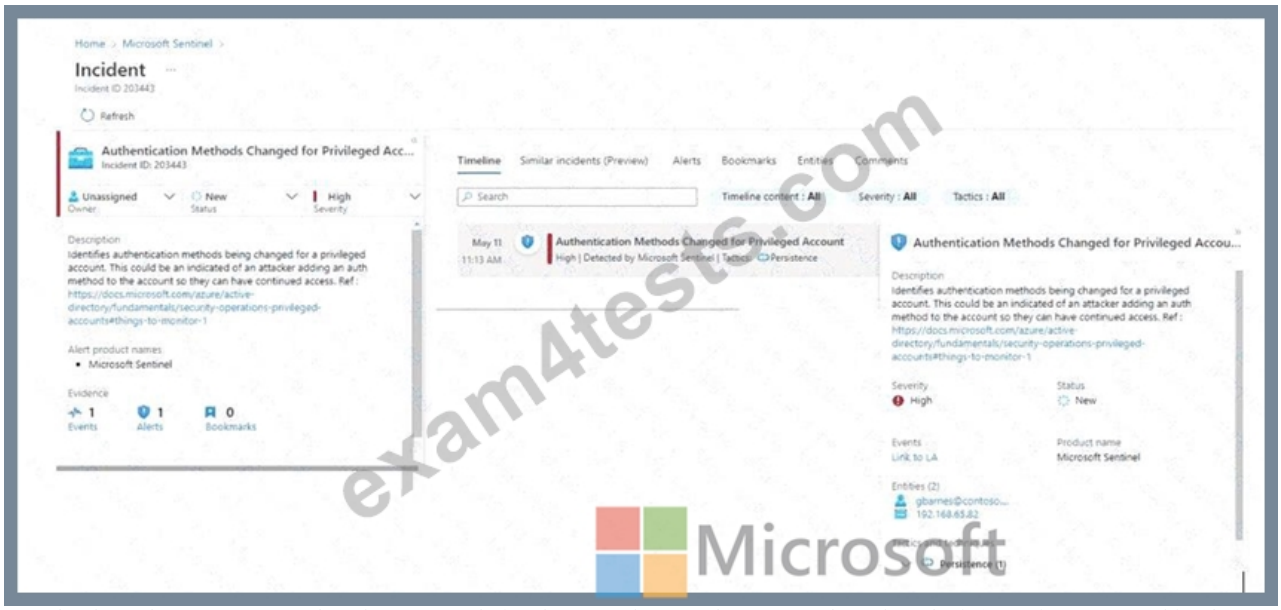
NEW QUESTION # 271
You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.
You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.
Which two actions should you perform? Each correct answer present part of the solution. create a KQL query that will i create a KQL query that will i NOTE: Each correct selection is worth one point.

- A. Create a Microsoft Cloud App Security connector.
- B. Create an Azure AD Identity Protection connector.
- C. Create a Microsoft incident creation rule based on Azure Security Center.
- D. Create custom rule based on the Office 365 connector templates.

Answer: B,D

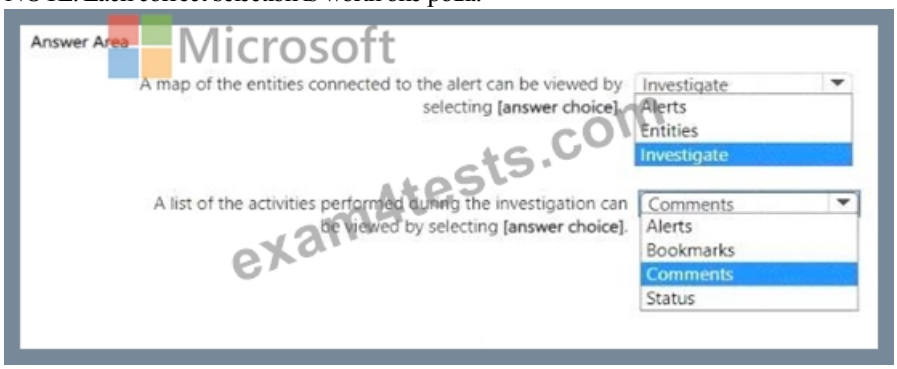
Explanation:
Explanation
To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:
Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.
Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules

NEW QUESTION # 272
You have a Microsoft Sentinel workspace.
A Microsoft Sentinel incident is generated as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in [the graphic.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION # 273

You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

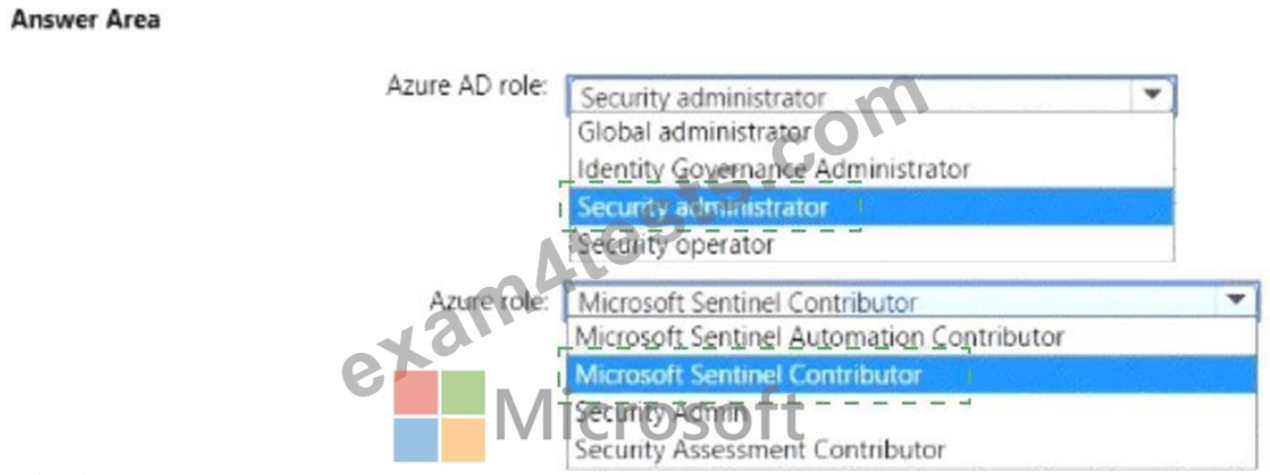
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD The solution must use The principle of least privilege.

Which roles should you assign to Used? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Explanation:

NEW QUESTION # 274

You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.

You have a team named Team1 that has a project named Project 1.

You need to identify any Project1 files that were stored on the team site of Team1 between February 1, 2023, and February 10, 2023.

Which KQL query should you run?

- A.
```
Project1(c:c)(date=2023-02-01..2023-02-10)
```
- B.
```
AuditLogs
| where Timestamp between (datetime(2023-02-01)..datetime(2023-02-10))
| where FileName contains "Project1"
```
- C.
```
AuditLogs
| where Timestamp > ago(10d)
| where FileName contains "Project1"
```

- D. 

Answer: B

NEW QUESTION # 275
.....

In order to cater to meet different needs of our customers, three versions of SC-200 exam bootcamp are available. Each version has its own advantages, and you can choose the most suitable one in accordance with your needs. Furthermore, SC-200 exam bootcamp is compiled by outstanding experts, therefore the quality and the accuracy can be guaranteed. Besides, we have the professional technicians to examine the website on a regular basis, hence a clean and safe shopping environment will be provided to you. You just need to buy the SC-200 Exam Dumps with ease.

Customizable SC-200 Exam Mode: https://www.exam4tests.com/SC-200-valid-braindumps.html

- The Microsoft SC-200 exam dumps are similar to real exam questions □ The page for free download of ➡ SC-200 □□□ on ▸ www.getvalidtest.com ◂ will open immediately □Real SC-200 Question
- 2025 Free SC-200 Practice | The Best 100% Free Customizable Microsoft Security Operations Analyst Exam Mode □ The page for free download of " SC-200 " on 【 www.pdfvce.com 】 will open immediately □Reliable SC-200 Study Plan
- SC-200 Official Practice Test □ SC-200 Best Vce □ Exam Dumps SC-200 Collection □ Copy URL ✔ www.examcollectionpass.com □✔□ open and search for □ SC-200 □ to download for free □Exam SC-200 Duration
- Free SC-200 Practice - Get Tagged as SC-200 Certified In No Time □ Go to website ➤ www.pdfvce.com □ open and search for ➤ SC-200 □ to download for free □SC-200 Valid Exam Camp Pdf
- Exam SC-200 Duration □ Test SC-200 Price □ SC-200 Certification Exam Cost □ Easily obtain free download of □ SC-200 □ by searching on [www.getvalidtest.com] □SC-200 Latest Test Questions
- 2025 Free SC-200 Practice | The Best 100% Free Customizable Microsoft Security Operations Analyst Exam Mode □ Search for ✔ SC-200 □✔□ and download it for free immediately on （ www.pdfvce.com ） □Exam SC-200 Duration
- SC-200 Exam Collection: Microsoft Security Operations Analyst - SC-200 Top Torrent - SC-200 Exam Cram □ Search for ▹ SC-200 ◃ and download it for free on ➥ www.pass4leader.com □ website □Exam SC-200 Duration
- Exam SC-200 Duration □ SC-200 Official Practice Test □ Exam SC-200 Duration □ Enter ➽ www.pdfvce.com □ □ and search for ☀ SC-200 □☀□ to download for free □New SC-200 Dumps Ebook
- The Microsoft SC-200 exam dumps are similar to real exam questions □ Enter ➽ www.real4dumps.com □ and search for ➥ SC-200 □ to download for free □SC-200 Exam PDF
- Hot SC-200 Questions □ SC-200 Valid Exam Camp Pdf □ SC-200 Test Prep □ Search for ➡ SC-200 □□□ and download it for free immediately on 《 www.pdfvce.com 》 □Reliable SC-200 Study Plan
- Free SC-200 Practice - Get Tagged as SC-200 Certified In No Time □ Open website 【 www.testsdumps.com 】 and search for ▸ SC-200 ◂ for free download □Hot SC-200 Questions
- kareyed271.develop-blog.com, 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, tedcole945.bloginder.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, training.siyashayela.com, academy.makeskilled.com, techavally.com, www.wcs.edu.eu, Disposable vapes

BTW, DOWNLOAD part of Exam4Tests SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=1GcSicQUd7sIpCuRB3B0Be05292-9R-t5