Latest Microsoft SC-200 Questions, SC-200 Reliable Dumps

P.S. Free & New SC-200 dumps are available on Google Drive shared by Actual4Cert: https://drive.google.com/open?id=128mN8aSyFLr8budvfPNBwxbQGwcKxJpZ

Some candidates may be afaind of the difficult questions in the SC-200 study materials for they are hard to be understood and memorized. But if you want to pass the exam perfectly, then you have to pay more attention on them. You must cultivate the good habit of reviewing the difficult parts of our SC-200 Practice Guide, which directly influences your passing rate. What is more, our experts never stop researching the questions of the real SC-200 exam. So our SC-200 exam questons are always the latest for you to download.

Microsoft SC-200, also known as Microsoft Security Operations Analyst certification exam, is designed for professionals who want to validate their skills in security operations center (SOC) roles. Microsoft Security Operations Analyst certification exam focuses on the knowledge and skills required to detect, respond to, and remediate security incidents using Microsoft products and services. By passing the SC-200 exam, candidates can prove their expertise in monitoring, analyzing, and responding to security threats.

To become certified in Microsoft SC-200, candidates must possess a strong understanding of Microsoft security technologies, including Azure Sentinel, Microsoft Defender for Endpoint, and Microsoft Cloud App Security. SC-200 exam includes a mix of multiple-choice questions, case studies, and hands-on tasks that test the candidate's ability to identify and respond to various security incidents. Successful candidates will need to demonstrate their ability to triage incidents, investigate potential security breaches, and identify and implement appropriate remediation measures. Overall, the Microsoft SC-200 Certification is a valuable credential for security analysts who want to advance their careers and demonstrate their expertise in Microsoft security technologies.

Microsoft SC-200 exam is designed to test candidates' knowledge and skills in various areas of security operations. SC-200 exam covers topics such as threat management, vulnerability management, incident response, security operations management, and data governance and compliance. Candidates are required to demonstrate their ability to use various security tools and technologies, including Microsoft Defender for Endpoint, Azure Sentinel, and Microsoft 365 Defender.

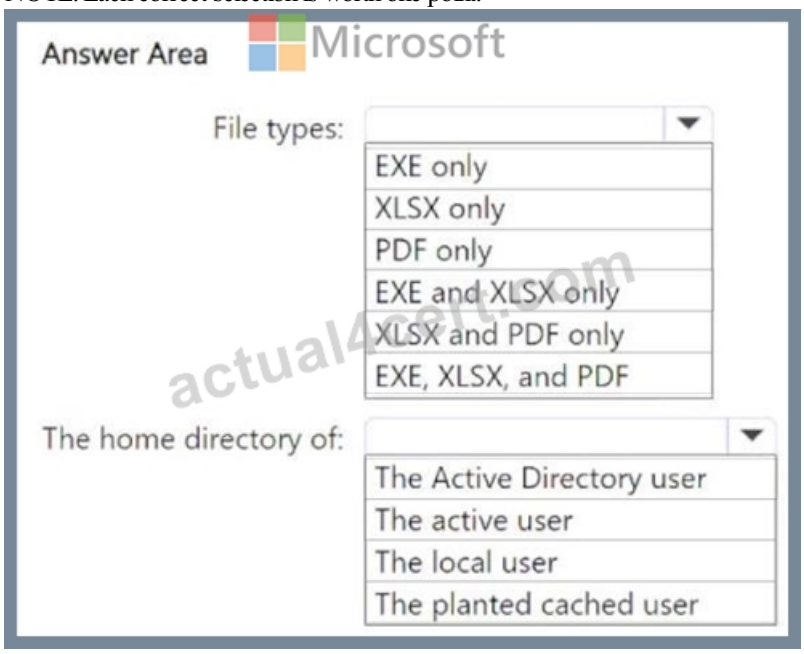
>> Latest Microsoft SC-200 Questions <<

SC-200 Reliable Dumps & SC-200 Exam Review

Feedbacks of many IT professionals who have passed Microsoft certification SC-200 exam prove that their successes benefit from Actual4Cert's help. Actual4Cert's targeted test practice questions and answers to gave them great help, which save their valuable time and energy, and allow them to easily and smoothly pass their first Microsoft Certification SC-200 Exam. So Actual4Cert a website worthy of your trust. Please select Actual4Cert, you will be the next successful IT person. Actual4Cert will help you achieve your dream.

Microsoft Security Operations Analyst Sample Questions (Q192-Q197):

NEW QUESTION # 192
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You are implementing a deception rule.
You need to provide a custom lure file.
For the custom lure, you set Planting path to HOME.
Which types of files can you use for the custom lure, and in which home directory should the file be located on a device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

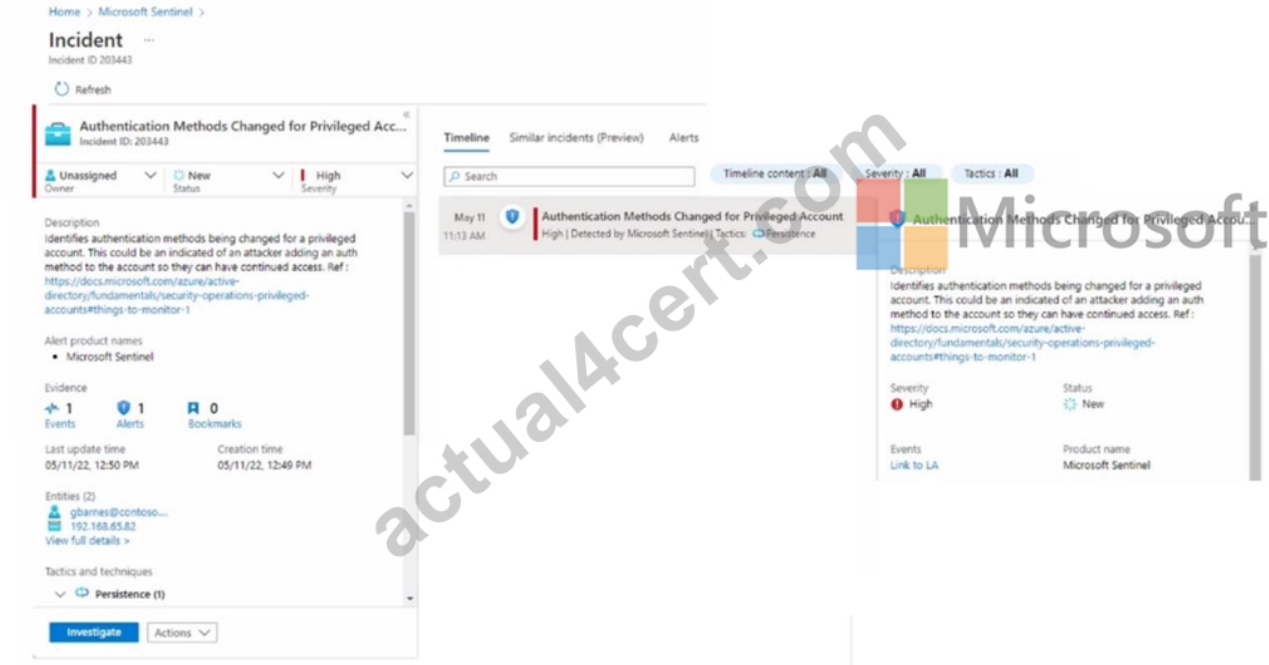
File types:

- EXE only
- XLSX only
- PDF only
- EXE and XLSX only
- XLSX and PDF only
- EXE, XLSX, and PDF

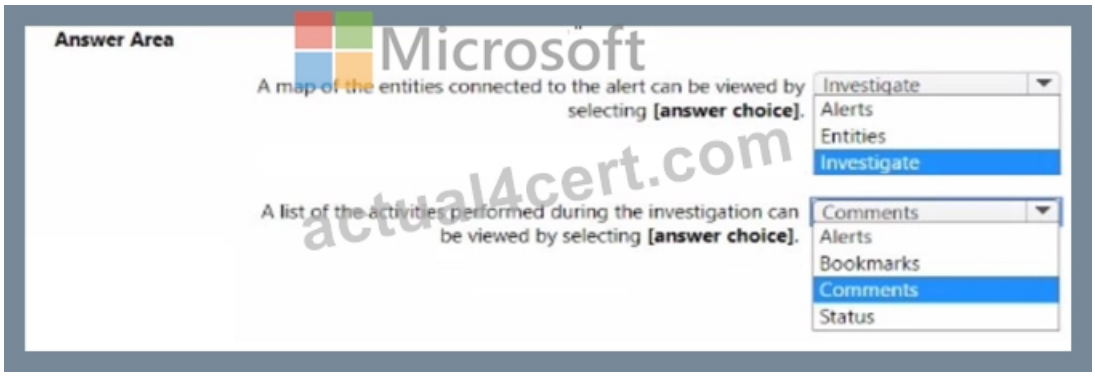
The home directory of:

- The Active Directory user
- The active user
- The local user
- The planted cached user

NEW QUESTION # 193
You have a Microsoft Sentinel workspace.
A Microsoft Sentinel incident is generated as shewn in the following exhibit.



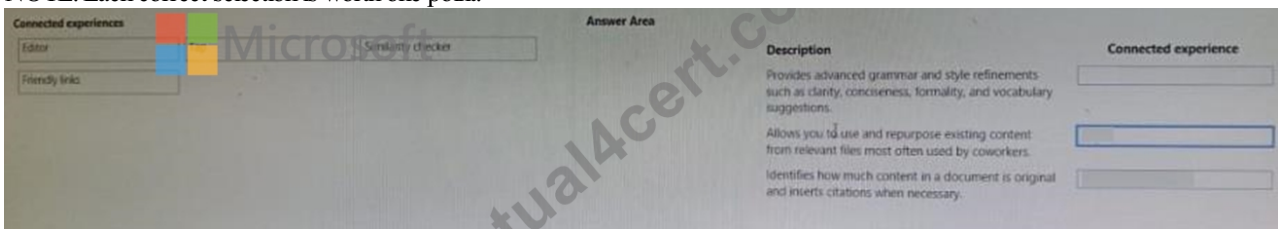
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



Answer:

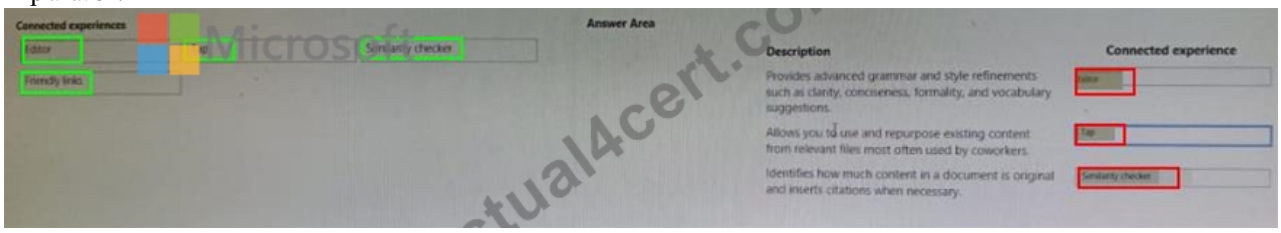
Explanation:

NEW QUESTION # 194
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



NEW QUESTION # 195
You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Incidents
- C. Threat intelligence
- D. Analytics

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

NEW QUESTION # 196
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

- A. a URL/domain indicator that has Action set to
- B. a URL/domain indicator that has Action set to
- C. a certificate indicator that has Action set to Alert and block
- D. a file hash indicator that has Action set to Alert and block

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

NEW QUESTION # 197
.....

Likewise, Web-Based Microsoft SC-200 exam questions are supported by all the major browsers like Chrome, Opera, Safari, Firefox, and IE. In the same way, the Web-based Microsoft Security Operations Analyst pdf exam requires no special plugin. Lastly, the web-based Microsoft Security Operations Analyst (SC-200) practice exam is customizable and requires an active Internet connection.

- Authorized Latest SC-200 Questions - Guaranteed Microsoft SC-200 Exam Success with The Best SC-200 Reliable Dumps □ Go to website ▹ www.vceengine.com ◃ open and search for ➠ SC-200 □ to download for free □SC-200 Test Cram Pdf
- lucyvhjv248151.blogars.com, www.stes.tyc.edu.tw, mysocialfeeder.com, inesatvn536517.blogozz.com, sahiladju031827.onzeblog.com, jayusry936201.mywikiparty.com, neilsvlu177019.vblogetin.com, ragingbookmarks.com, 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, dopementor.com, Disposable vapes

P.S. Free & New SC-200 dumps are available on Google Drive shared by Actual4Cert: https://drive.google.com/open?id=128mN8aSyFLr8budvfPNBwxbQGwcKxJpZ