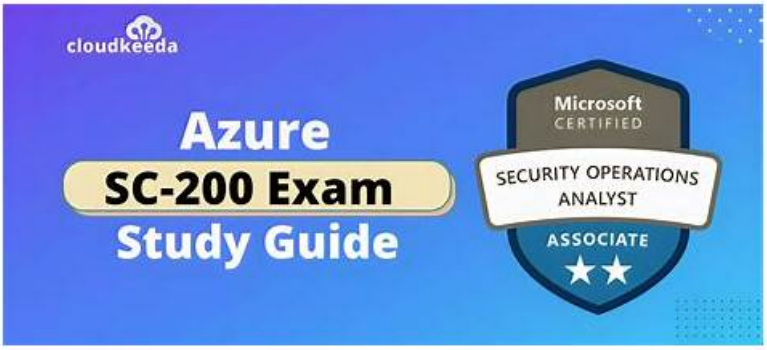
Certification SC-200 Test Questions - Latest SC-200 Test Dumps



P.S. Free 2025 Microsoft SC-200 dumps are available on Google Drive shared by VerifiedDumps: https://drive.google.com/open?id=1wNCSxieOJWibDdLsyZ5F8yDLuKmD4nDI

Therefore, you have the option to use Microsoft SC-200 PDF questions anywhere and anytime. VerifiedDumps Microsoft Security Operations Analyst (SC-200) dumps are designed according to the Microsoft Security Operations Analyst (SC-200) certification exam standard and have hundreds of questions similar to the actual SC-200 Exam. VerifiedDumps Microsoft web-based practice exam software also works without installation.

The PDF version of our SC-200 study tool is very practical, which is mainly reflected on the special function. As I mentioned above, our company are willing to provide all people with the demo for free. You must want to know how to get the trial demo of our SC-200 question torrent; the answer is the PDF version. You can download the free demo form the PDF version of our SC-200 exam torrent. Maybe you think it does not prove the practicality of the PDF version, do not worry, we are going to tell us another special function about the PDF version of our SC-200 Study Tool. If you download our study materials successfully, you can print our study materials on pages by the PDF version of our SC-200 exam torrent. We believe these special functions of the PDF version will be very useful for you to prepare for your exam. We hope that you will like the PDF version of our SC-200 question torrent.

>> Certification SC-200 Test Questions <<

Latest Microsoft SC-200 Test Dumps - Valid SC-200 Test Prep

If you would like to use all kinds of electronic devices to prepare for the SC-200 SC-200 exam, then I am glad to tell you that our online app version is definitely your perfect choice. In addition, another strong point of the online app version is that it is convenient for you to use even though you are in offline environment. In other words, you can prepare for your SC-200 Exam with under the guidance of our training materials anywhere at any time. Just take action to purchase we would be pleased to make you the next beneficiary of our SC-200 exam practice.

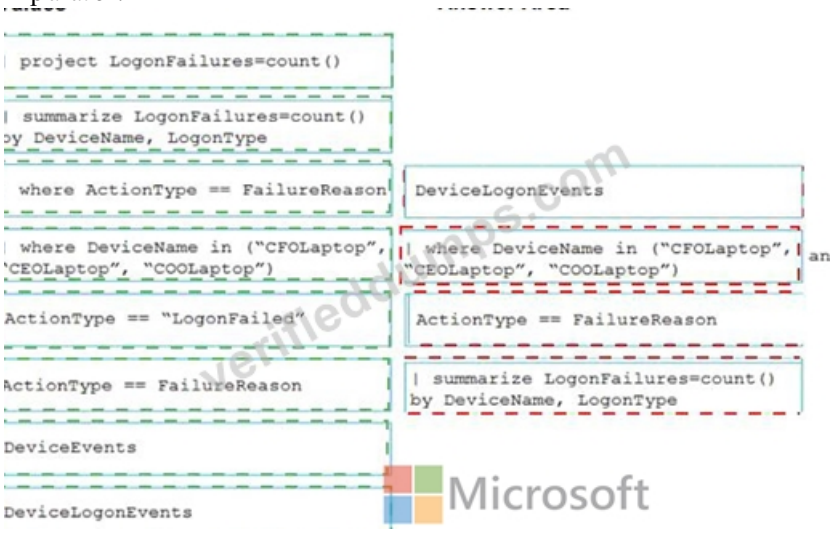
Microsoft Security Operations Analyst certification exam, also known as SC-200, is designed for security professionals who are responsible for managing and monitoring security solutions in an organization. Microsoft Security Operations Analyst certification validates the skills and knowledge required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

Microsoft Security Operations Analyst Sample Questions (Q241-Q246):

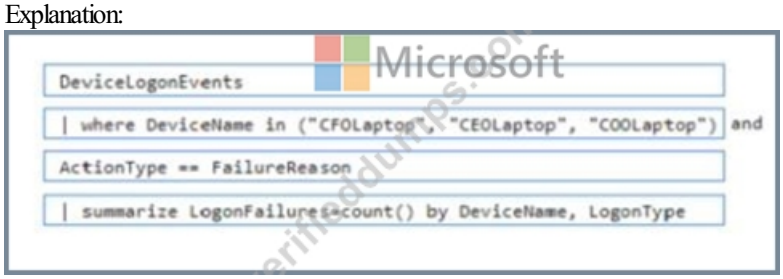
NEW QUESTION # 241
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point

Answer:

Explanation:



Explanation:



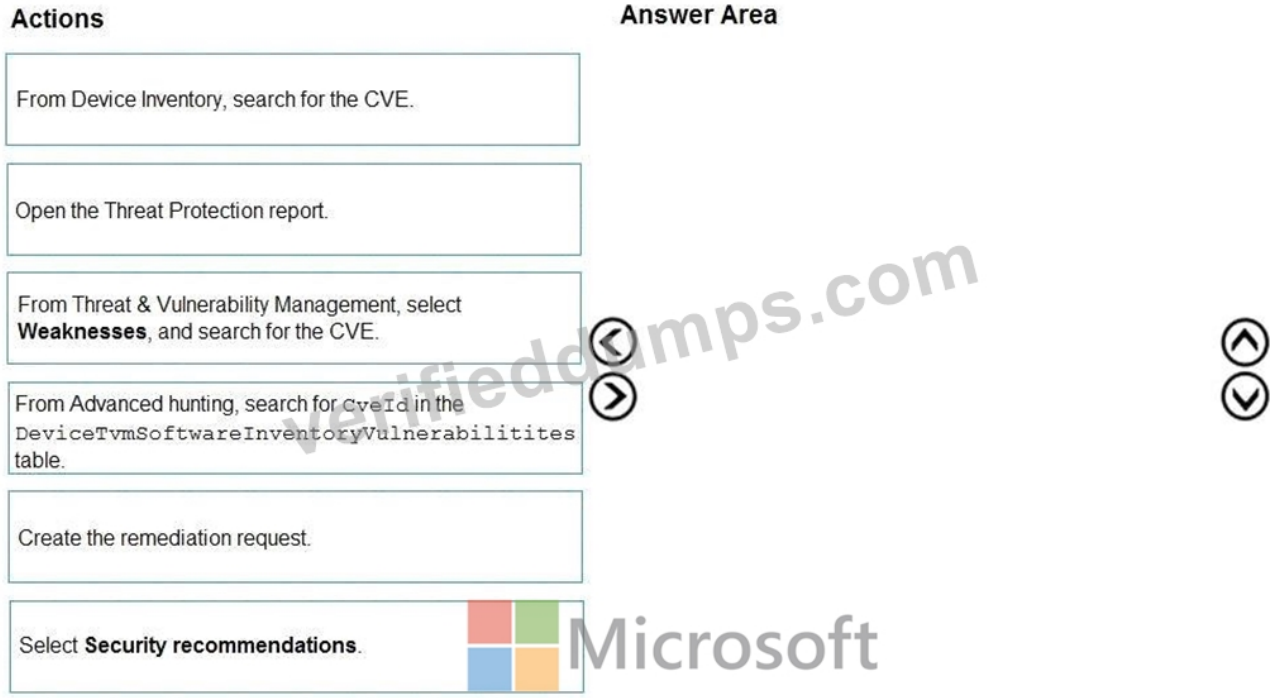
NEW QUESTION # 242

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.

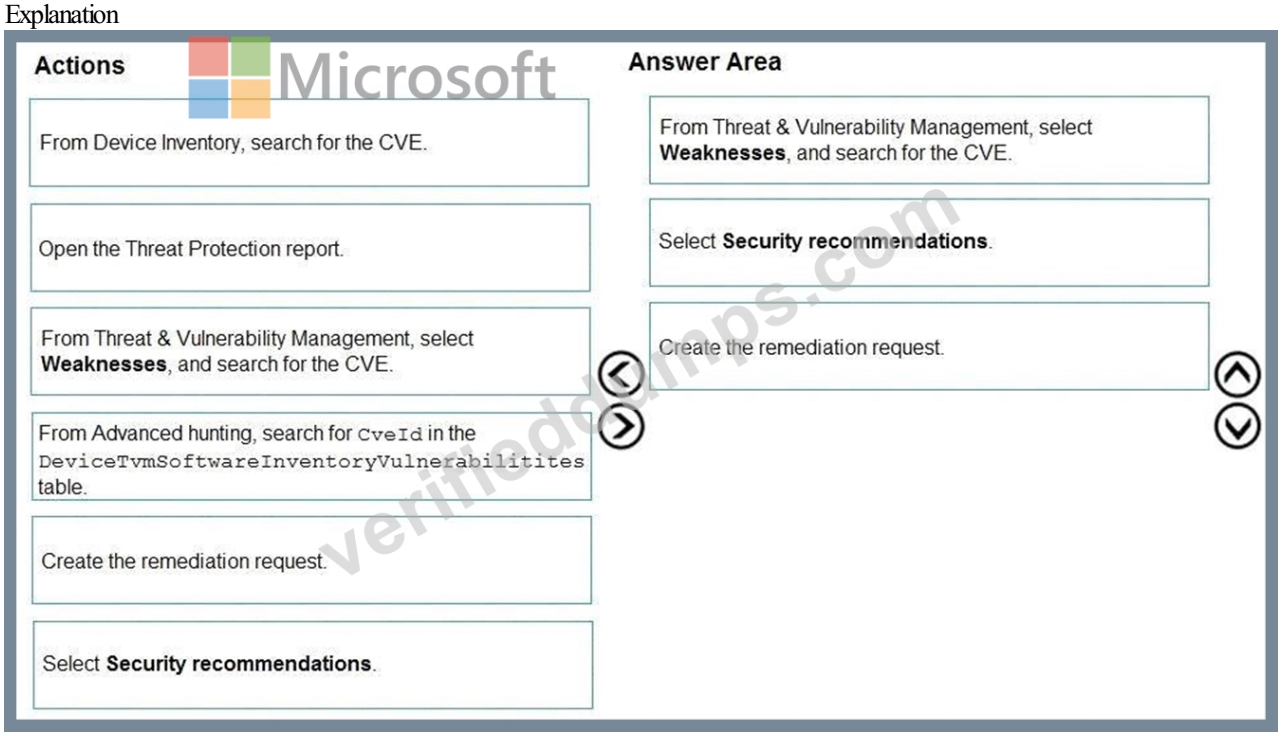
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer

area and arrange them in the correct order.



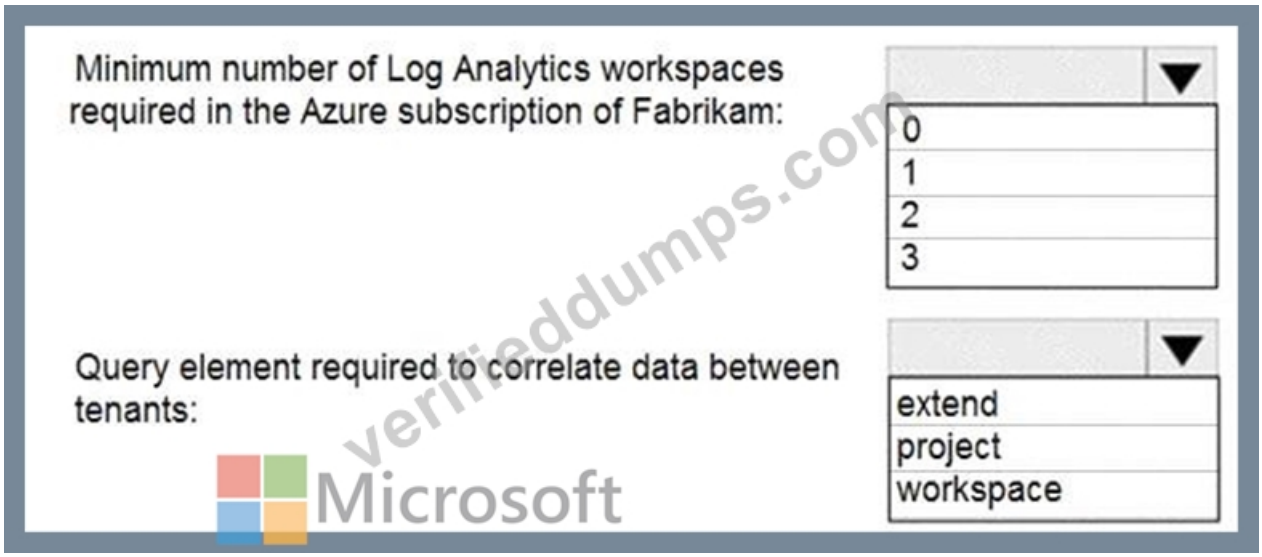
Answer:

Explanation:
Explanation



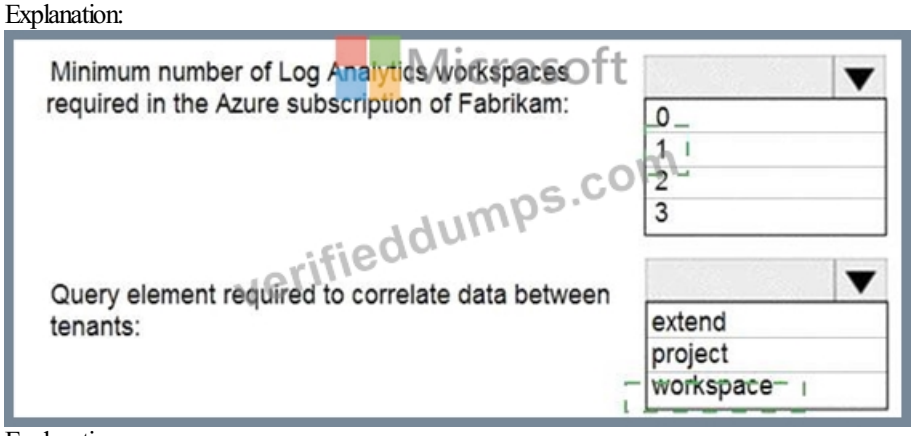
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps

NEW QUESTION # 243
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

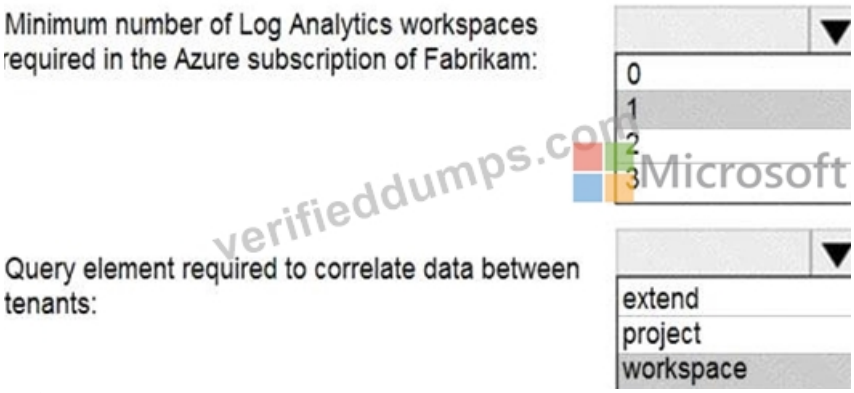


Answer:

Explanation:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Topic 2, Litware inc.

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the

case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

The principle of least privilege must be used whenever possible.

Costs must be minimized, as long as all other requirements are met.

Logs collected by Log Analytics must provide a full audit trail of user activities.

All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.

Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

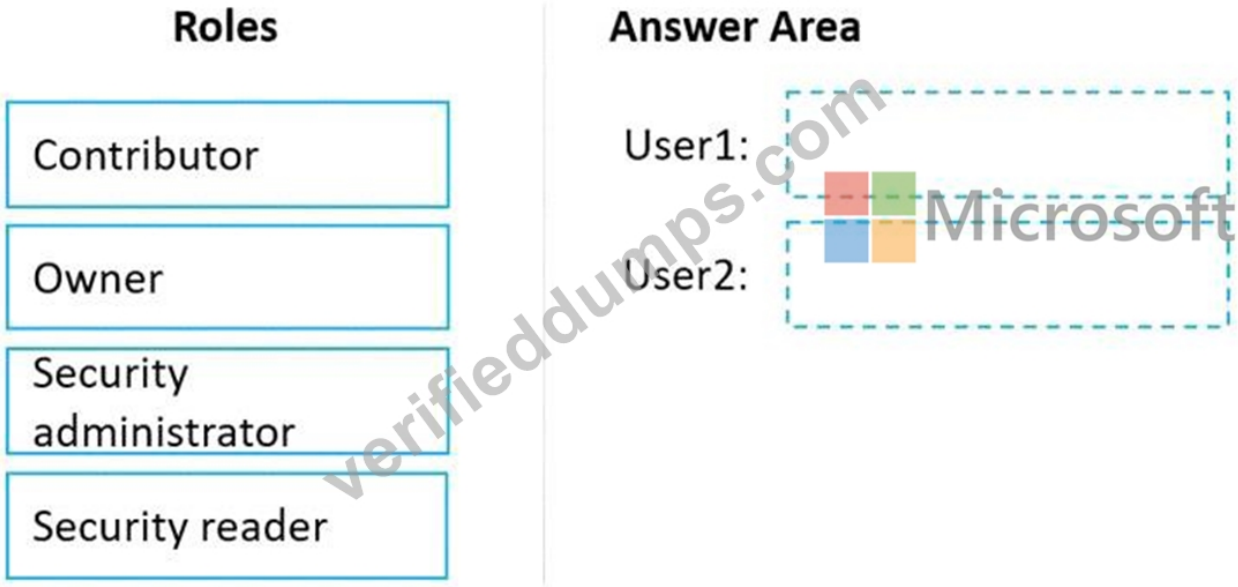
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION # 244
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

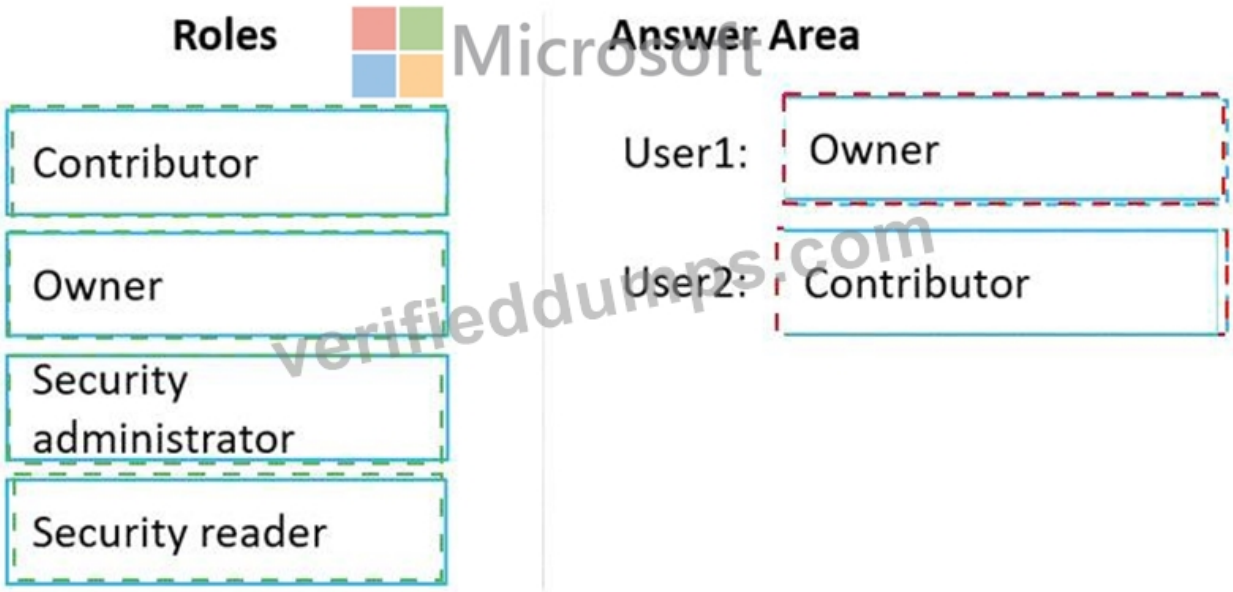
User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



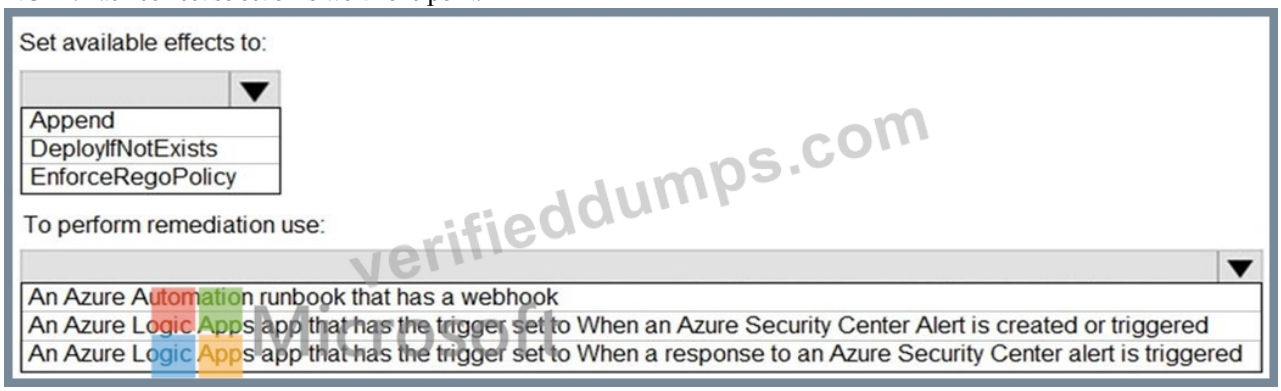
Answer:

Explanation:



Explanation
Box 1: Owner
Only the Owner can assign initiatives.
Box 2: Contributor
Only the Contributor or the Owner can apply security recommendations.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

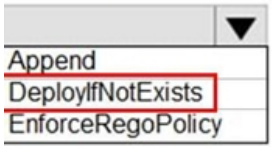
NEW QUESTION # 245
You have an Azure subscription that uses Azure Defender.
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.
You need to create an Azure policy that will perform threat remediation automatically.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



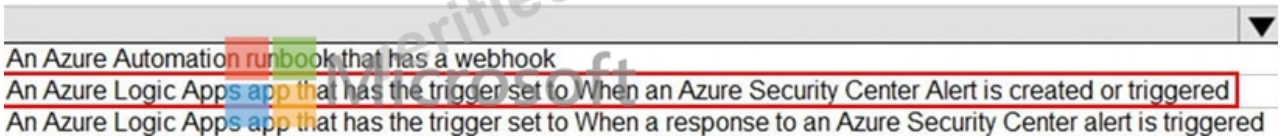
Answer:

Explanation:

Set available effects to:



To perform remediation use:



Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION # 246
.....

Whether you are good at learning or not, passing the exam can be a very simple and enjoyable matter together with our SC-200 practice engine. As a professional multinational company, we fully take into account the needs of each user when developing our SC-200 Exam Braindumps. For example, in order to make every customer can purchase at ease, our SC-200 preparation quiz will provide users with three different versions for free trial, corresponding to the three official versions.

Latest SC-200 Test Dumps: https://www.verifieddumps.com/SC-200-valid-exam-braindumps.html

- 100% Pass SC-200 - Useful Certification Microsoft Security Operations Analyst Test Questions □ Open ▷ www.torrentvalid.com ◁ and search for （ SC-200 ） to download exam materials for free □Most SC-200 Reliable Questions
- New SC-200 Test Dumps □ Valid Dumps SC-200 Book □ SC-200 Exam Score □ Search for 「 SC-200 」 and easily obtain a free download on ➽ www.pdfvce.com □ □SC-200 Latest Exam Discount
- Professional Certification SC-200 Test Questions - Leader in Certification Exams Materials - Trustworthy Latest SC-200 Test Dumps □ ➠ www.itcerttest.com □ is best website to obtain 【 SC-200 】 for free download □Valid SC-200 Real Test
- Professional Certification SC-200 Test Questions - Leader in Certification Exams Materials - Trustworthy Latest SC-200 Test Dumps □ Search for ➠ SC-200 □ on ➥ www.pdfvce.com □ immediately to obtain a free download □Valid Dumps SC-200 Book
- Most SC-200 Reliable Questions □ Valid SC-200 Real Test □ High SC-200 Passing Score □ Download ➥ SC-200 □ for free by simply searching on ➥ www.testkingpdf.com □ □Most SC-200 Reliable Questions
- SC-200 practice materials - SC-200 guide torrent: Microsoft Security Operations Analyst - SC-200 study guide □ Open ☀ www.pdfvce.com □☀□ enter ☀ SC-200 □☀□ and obtain a free download □Exam Dumps SC-200 Pdf
- SC-200 Test Dumps Demo □ Valid SC-200 Test Simulator □ SC-200 Authorized Test Dumps □ Open □ www.passtestking.com □ and search for ➽ SC-200 □ to download exam materials for free □Frequent SC-200 Updates
- SC-200 Test Dumps Demo □ Frequent SC-200 Updates □ Exam Dumps SC-200 Pdf □ Download ▸ SC-200 ◂ for free by simply searching on 【 www.pdfvce.com 】 □New SC-200 Test Dumps
- Frequent SC-200 Updates □ SC-200 Exam Score □ SC-200 Test Dumps Demo □ Download ▸ SC-200 ◂ for free by simply entering 【 www.prep4sures.top 】 website □High SC-200 Passing Score
- Frequent SC-200 Updates □ SC-200 Latest Exam Discount □ SC-200 Useful Dumps □ Immediately open ▸ www.pdfvce.com ◂ and search for 《 SC-200 》 to obtain a free download □SC-200 Authorized Test Dumps
- 2025 100% Free SC-200 –Valid 100% Free Certification Test Questions | Latest Microsoft Security Operations Analyst Test Dumps □ Search for ✔ SC-200 □✔□ and easily obtain a free download on ➥ www.examcollectionpass.com □ □Valid Dumps SC-200 Book
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, helpingmummiesanddaddiesagencytt.com, 40bbk.com, studywithjoydeep.com, ncon.edu.sa, mikemil988.spintheblog.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, myportal.utt.edu.tt, Disposable vapes

BONUS!!! Download part of VerifiedDumps SC-200 dumps for free: https://drive.google.com/open?id=1wNCSxieOJWibDdLsyZ5F8yDLuKmD4nDI