New SC-200 Test Camp | SC-200 Exam Experience

P.S. Free 2025 Microsoft SC-200 dumps are available on Google Drive shared by PDFDumps: https://drive.google.com/open?id=17LqmG74rItlQvmCCW-lNd8DY7H3OnkJ5

It is an important process that filling in the correct mail address in order that it is easier for us to send our SC-200 study guide to you after purchase, therefore, this personal message is particularly important. We are selling virtual SC-200 learning dumps, and the order of our SC-200 training materials will be immediately automatically sent to each purchaser's mailbox according to our system. It is very fast and convenient to have our SC-200 practice questions.

Microsoft SC-200 (Microsoft Security Operations Analyst) Certification Exam is designed to test the knowledge and skills of security professionals in performing threat protection, incident response, and other security operations tasks using Microsoft security technologies. Microsoft Security Operations Analyst certification exam is intended for those who have expertise in security operations and experience working with Microsoft Azure Sentinel, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Cloud App Security.

>> New SC-200 Test Camp <<

Hot New SC-200 Test Camp 100% Pass | Pass-Sure SC-200 Exam Experience: Microsoft Security Operations Analyst

A dedicated team is accessible for PDFDumps customers. One can reach our 24/7 customer support team to resolve their queries. Moreover, our team will also assist users if they face any kind of trouble while using above-mentioned formats of SC-200 practice material. We will offer you a refund guarantee (terms and conditions apply) as saving your money is our priority. Additionally, we offer up to 1 year of free updates and free demo of the SC-200 product. Order Microsoft SC-200 exam questions now and get excellent these offers.

Microsoft Security Operations Analyst Sample Questions (Q78-Q83):

NEW QUESTION # 78
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.

You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct answer is worth one point.

- A. From Defender for Cloud, configure auto-provisioning.
- B. Onboard the virtual machines to Microsoft Defender for Endpoint.
- C. From Defender for Cloud, configure the AWS connector.
- D. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.
- E. From Defender for Cloud, enable agentless scanning.

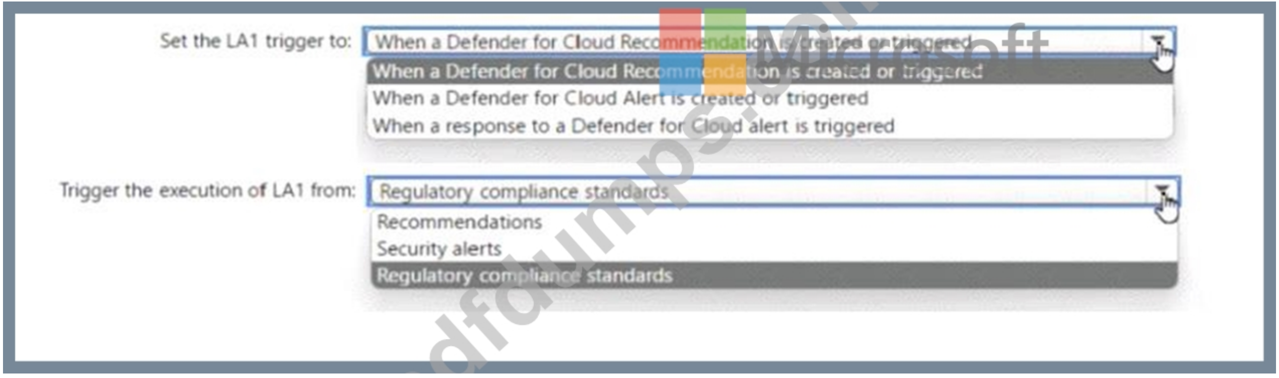
Answer: A,C

NEW QUESTION # 79
You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You plan to create a hunting query from Microsoft Defender.
You need to create a custom tracked query that will be used to assess the threat status of the subscription.
From the Microsoft 365 Defender portal, which page should you use to create the query?

- A. Advanced Hunting
- B. Explorer
- C. Policies & rules
- D. Threat analytics

Answer: A

NEW QUESTION # 80
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud.
You need to test LA1 in Defender for Cloud.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered

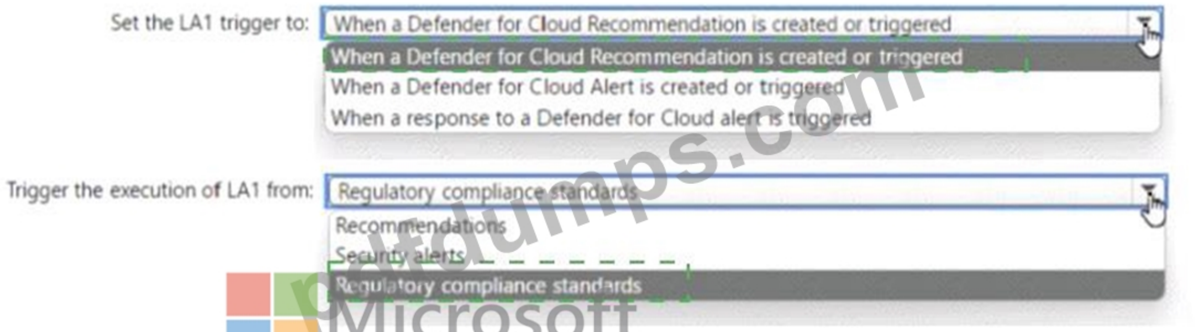
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from: Regulatory compliance standards

Recommendations
Security alerts
Regulatory compliance standards

Answer:

Explanation:



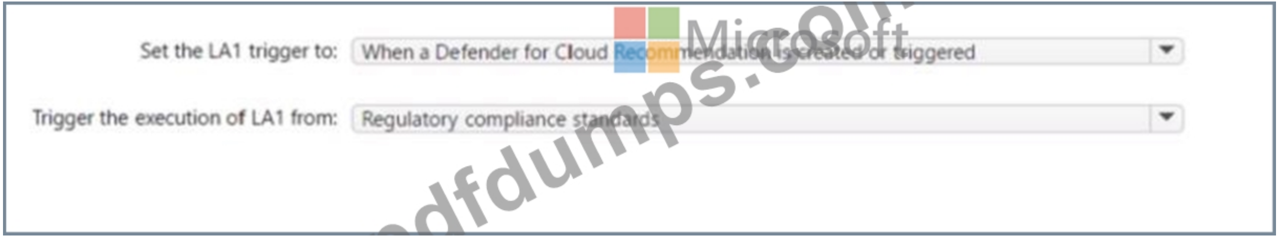
Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered

When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from: Regulatory compliance standards

Recommendations
Security alerts
Regulatory compliance standards

Explanation



Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered

Trigger the execution of LA1 from: Regulatory compliance standards

NEW QUESTION # 81

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

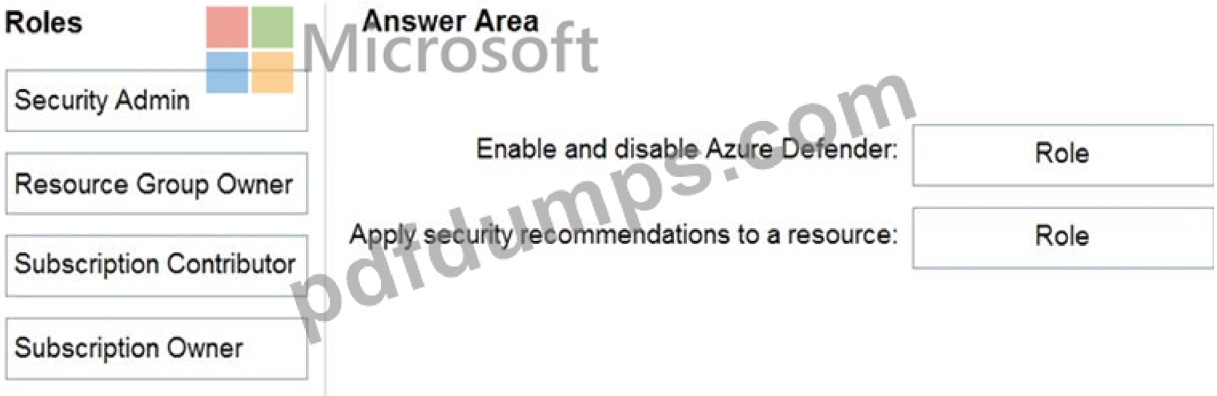
Enable and disable Azure Defender.

Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. 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.

NOTE: Each correct selection is worth one point.

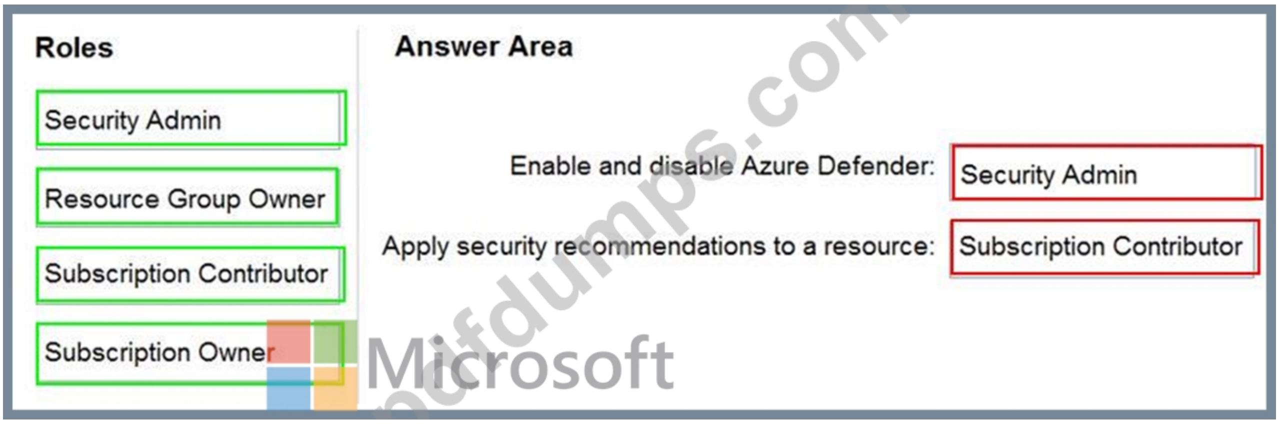


Enable and disable Azure Defender: Role

Apply security recommendations to a resource: Role

Answer:

Explanation:



Roles

Security Admin

Resource Group Owner

Subscription Contributor

Subscription Owner

Answer Area

Enable and disable Azure Defender: Security Admin

Apply security recommendations to a resource: Subscription Contributor

Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

NEW QUESTION # 82

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

Answer: A,B

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 # 83

......

You can choose the most suitable and convenient one for you. The web-based SC-200 practice exam is compatible with all operating systems. It is a browser-based Microsoft SC-200 Practice Exam that works on all major browsers. This means that you won't have to worry about installing any complicated software or plug-ins.

SC-200 Exam Experience: https://www.pdfdumps.com/SC-200-valid-exam.html www.exams4collection.com } immediately to obtain a free download □Latest SC-200 Study Materials

- Test SC-200 Collection Pdf □ Latest SC-200 Study Materials □ Test SC-200 Collection Pdf □ Copy URL ➡ www.pdfvce.com □□□ open and search for □ SC-200 □ to download for free □New SC-200 Exam Pdf
- Exam Dumps SC-200 Free □ Latest SC-200 Dumps Questions ↕ Exam Dumps SC-200 Free □ Open 「 www.testsdumps.com 」 enter ▷ SC-200 ◁ and obtain a free download □Exam SC-200 Actual Tests
- Microsoft Security Operations Analyst sure pass dumps - SC-200 actual training pdf □ Easily obtain free download of 【 SC-200 】 by searching on ▷ www.pdfvce.com ◁ □Latest SC-200 Study Materials
- Certification SC-200 Exam Cost □ Latest SC-200 Dumps Questions ☃ SC-200 Real Dumps □ Search for 「 SC-200 」 and download exam materials for free through ➥ www.prep4away.com □ □Exam SC-200 Actual Tests
- Practice SC-200 Engine □ SC-200 Pass Rate □ Valid SC-200 Exam Topics □ Search for ✔ SC-200 □✔□ and download it for free immediately on 【 www.pdfvce.com 】 □Valid SC-200 Exam Topics
- Test SC-200 Collection Pdf □ Valid SC-200 Test Syllabus ✔ Test SC-200 Collection Pdf □ Simply search for “ SC-200 ” for free download on □ www.exams4collection.com □ □SC-200 Test Objectives Pdf
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.yxsensing.net, 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, www.stes.tyc.edu.tw, ncon.edu.sa, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of PDFDumps SC-200 dumps for free: https://drive.google.com/open?id=17LqmG74rItlQvmCCW-lNd8DY7H3OnkJ5