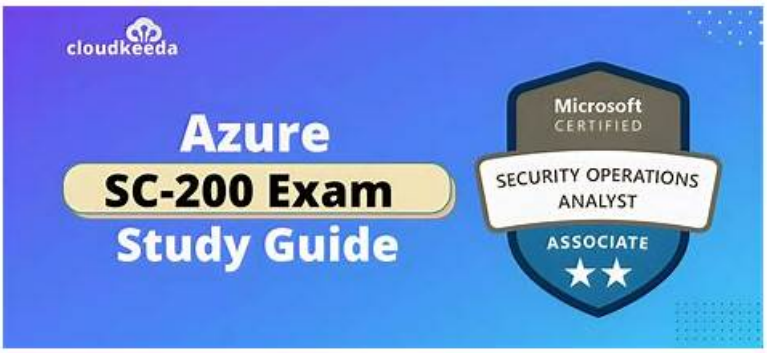
Valid SC-200 Study Guide - Exam SC-200 Consultant



DOWNLOAD the newest Exam4Labs SC-200 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1J-Q7EFRdkmq94xJZ9FqVX7ip7FJrd3OQ

Exam4Labs experts have also developed Microsoft Security Operations Analyst (SC-200) test simulation software for you to assess and improve yourself. This is especially useful for intensive preparation and revision. It will provide you with an Microsoft Security Operations Analyst (SC-200) exam environment and will give you real exam Microsoft SC-200 questions.

If you are looking to take the Microsoft SC-200 Exam, you should have a good understanding of security operations and be familiar with various security tools and technologies. You should also have experience in threat management, incident response, and vulnerability management. Additionally, you should have a good understanding of Microsoft's security solutions, including Microsoft 365 Defender and Azure Sentinel.

>> Valid SC-200 Study Guide <<

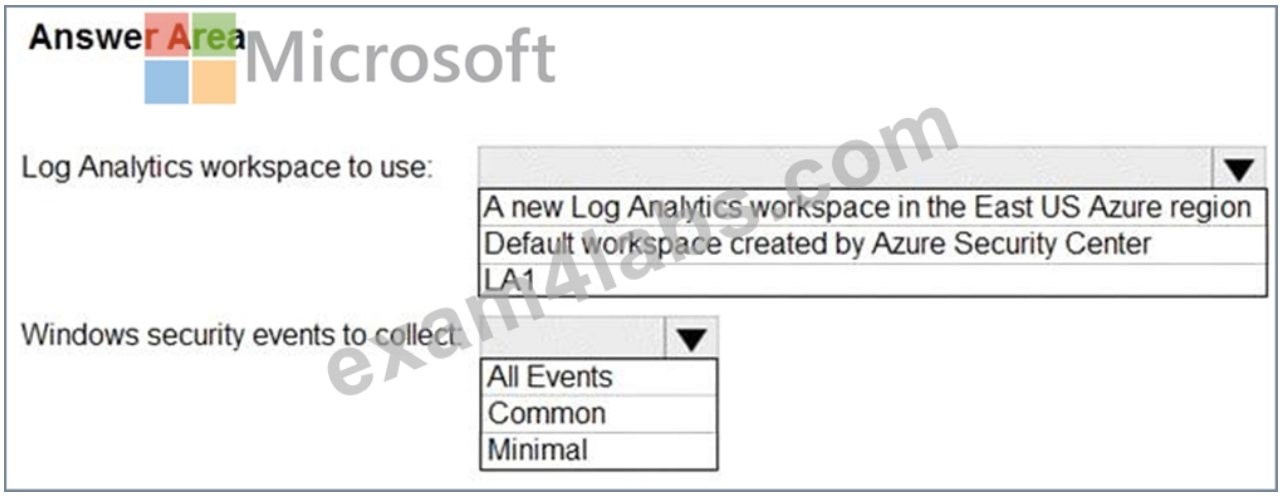
Pass Guaranteed Pass-Sure Microsoft - SC-200 - Valid Microsoft Security Operations Analyst Study Guide

If you intend to take the Microsoft SC-200 exam to open doors to high-paying jobs, you need an authentic Microsoft SC-200 practice exam material to get a passing score on the first attempt. Many people do not find a platform that is credible to purchase updated Microsoft SC-200 prep material. This leads to a waste of time and money, and ultimately failure in the SC-200 exam.

Microsoft Security Operations Analyst, or SC-200, certification exam is designed for security professionals who are responsible for monitoring and responding to security incidents in Microsoft environments. SC-200 exam tests the candidate's knowledge and skills in various areas such as threat management, vulnerability management, incident response, and compliance. Passing the SC-200 Exam demonstrates that the candidate has the expertise required to protect Microsoft environments from cyber threats.

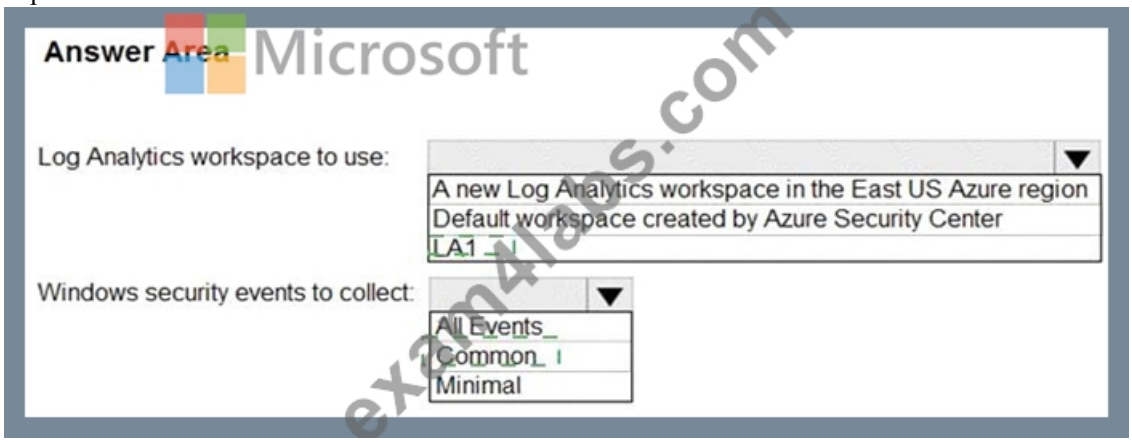
Microsoft Security Operations Analyst Sample Questions (Q353-Q358):

NEW QUESTION # 353
You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business 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.

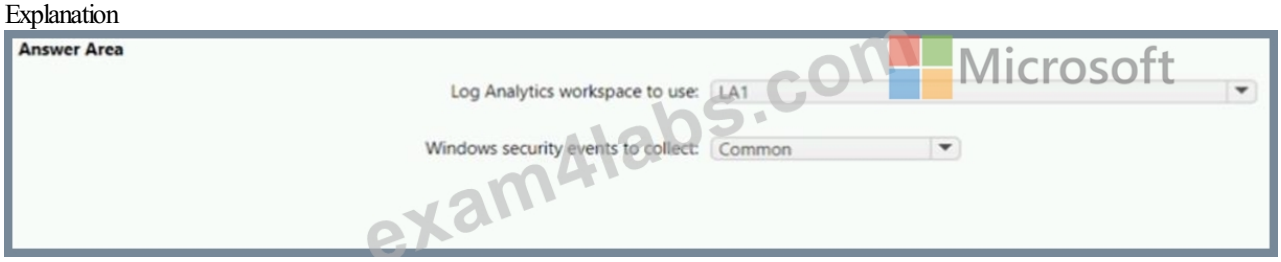


Answer:

Explanation:



Explanation



NEW QUESTION # 354

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.

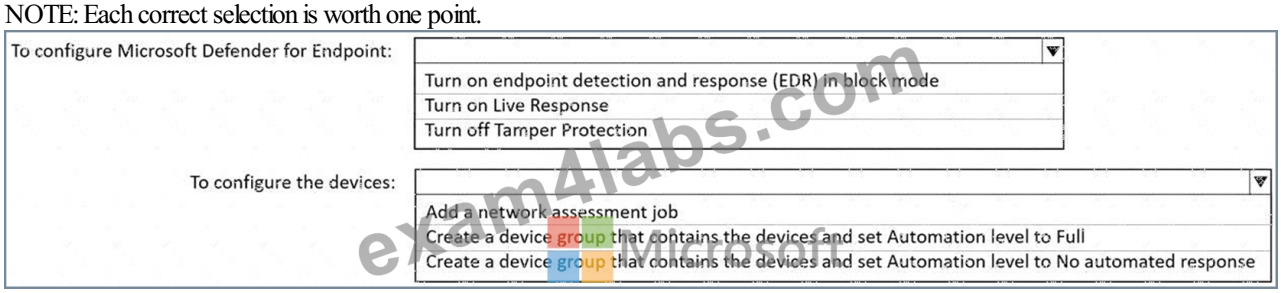
- A. Create custom rule based on the Office 365 connector templates.
- B. Create a Microsoft Cloud App Security connector.
- C. Create a Microsoft incident creation rule based on Azure Security Center.
- D. Create an Azure AD Identity Protection connector.

Answer: A,D

Explanation:

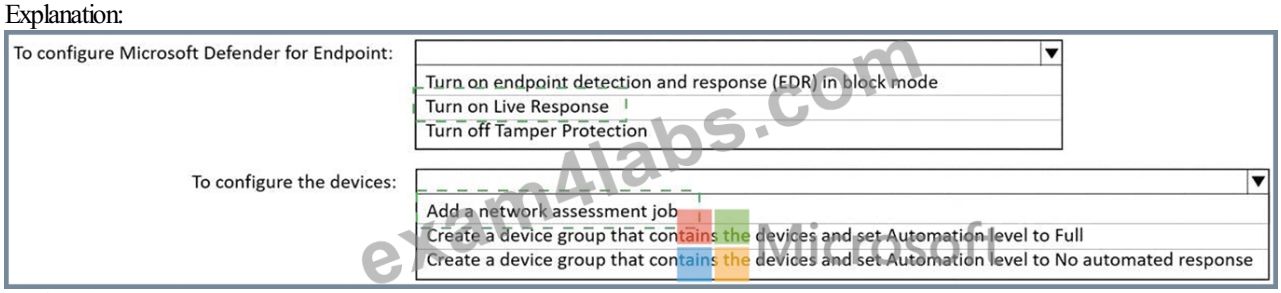
To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:
Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities 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 # 355
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Explanation:
Box 1: Turn on Live Response
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldw

NEW QUESTION # 356
You have a Microsoft Sentinel workspace named Workspacel that contains a table named CommonSecurityLog. You ingest logs into CommonSecurityLog. CommonSecurityLog has an average log ingestion time of five minutes.
You need to create an analytics rule that has a lookback period of seven minutes and uses the data in the CommonSecurityLog table. The solution must meet the following requirements:
* Prevent the same event from being processed twice.
* Minimize the number of missed events due to log ingestion delays.
How should you complete the KQL query that defines the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

When creating scheduled analytics rules in Microsoft Sentinel, you should account for ingestion delay so late-arriving events aren't missed, while also avoiding reprocessing the same events. The recommended pattern is to widen the TimeGenerated window by the expected delay and then gate results by ingestion_time() to include only data that actually arrived within the delay window:

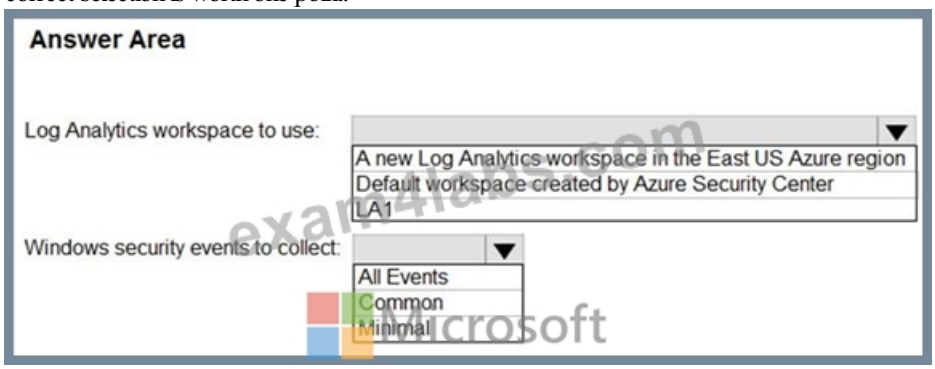
let ingestion_delay = 5min;
let rule_look_back = 7min;
CommonSecurityLog
| where TimeGenerated >= ago(ingestion_delay + rule_look_back) // cover late arrivals
| where ingestion_time() > ago(ingestion_delay) // only newly ingested data

* TimeGenerated >= ago(ingestion_delay + rule_look_back) ensures the query looks back 7 + 5 = 12 minutes, so events that were generated up to 7 minutes ago but arrived up to 5 minutes late are still captured.
* ingestion_time() > ago(ingestion_delay) limits results to items ingested in the last 5 minutes, preventing the same already-processed events from being picked up again on the next run, while minimizing misses due to late ingestion.

Thus, choose (ingestion_delay + rule_look_back) for the first blank and (ingestion_delay) for the second.

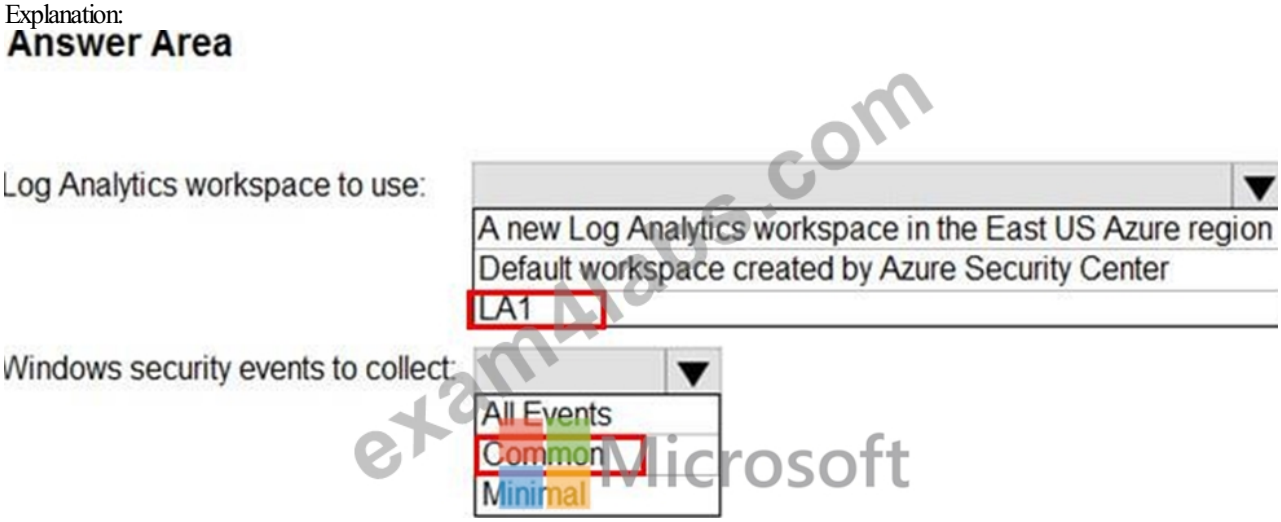
NEW QUESTION # 357

You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.



Answer:

Explanation:



NEW QUESTION # 358

.....

Exam SC-200 Consultant: https://www.exam4labs.com/SC-200-practice-torrent.html

- Exam Vce SC-200 Free □ SC-200 Latest Exam Materials □ SC-200 Trustworthy Exam Content □ Search for " SC-200 " on □ www.prepawayete.com □ immediately to obtain a free download □New SC-200 Test Practice
- SC-200 Mock Exams □ SC-200 Latest Exam Materials □ Latest SC-200 Cram Materials □ Enter ➥ www.pdfvce.com □ and search for （ SC-200 ） to download for free □SC-200 Clear Exam
- Top Features of www.vceengine.com Microsoft SC-200 Practice Questions File □ Search for ➽ SC-200 □ on ➥ www.vceengine.com □ immediately to obtain a free download □Reliable SC-200 Test Simulator
- 100% Pass SC-200 - Microsoft Security Operations Analyst –Reliable Valid Study Guide ↖ □ www.pdfvce.com □ is best website to obtain ⇛ SC-200 ⇚ for free download □Latest SC-200 Cram Materials
- New SC-200 Test Practice □ Practice SC-200 Questions ☯ SC-200 Valid Test Materials □ Search for 《 SC-200 》 on ▸ www.practicevce.com ◂ immediately to obtain a free download □SC-200 Valid Exam Simulator
- Reliable SC-200 Test Simulator □ SC-200 Valid Exam Simulator □ SC-200 Valid Braindumps Questions □ Search for 「 SC-200 」 and easily obtain a free download on ➥ www.pdfvce.com □ □Latest SC-200 Cram Materials
- SC-200 Trustworthy Exam Content □ Authorized SC-200 Certification □ SC-200 Exam Simulations □ Search for （ SC-200 ） and download exam materials for free through □ www.troytecdumps.com □ ↘SC-200 Latest Exam Materials
- SC-200 Test Braindumps: Microsoft Security Operations Analyst - SC-200 Quiz Materials - SC-200 Exam Torrent □ Search on □ www.pdfvce.com □ for 「 SC-200 」 to obtain exam materials for free download □SC-200 Exam Simulations
- Latest Upload Microsoft Valid SC-200 Study Guide: Microsoft Security Operations Analyst □ ⇛ www.pdfdumps.com ⇚ is best website to obtain ✔ SC-200 □✔□ for free download □New SC-200 Test Practice
- Top Features of Pdfvce Microsoft SC-200 Practice Questions File □ Copy URL （ www.pdfvce.com ） open and search for ▹ SC-200 ◃ to download for free □Free SC-200 Practice

- SC-200 Mock Exams □ Authorized SC-200 Certification □ New SC-200 Test Practice □ Copy URL ⇛ www.examcollectionpass.com ⇚ open and search for " SC-200 " to download for free □SC-200 Mock Exams
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, wisdomvalleyedu.in, kumu.io, lms.ait.edu.za, 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, 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, Disposable vapes

P.S. Free & New SC-200 dumps are available on Google Drive shared by Exam4Labs: https://drive.google.com/open?id=1J-Q7EFRdkmq94xJZ9FqVX7ip7FJrd3OQ