SC-200 Exam Questions & New SC-200 Dumps Questions

BONUS!!! Download part of ExamsLabs SC-200 dumps for free: https://drive.google.com/open?id=1NiirUyVQ8QxJkuuPwnp7yaC9btZrNbYq

Be certain about what you believe and consistent in what you say. If you intend to pass Microsoft SC-200 exam, you must take prompt action. Which is the best for your reference on the website? If you don't know how to choose your reference materials, we commend our ExamsLabs Microsoft SC-200 Study Guide to you. ExamsLabs Microsoft SC-200 certification training materials is the most complete. There is another advantage: we can provide you with free update for a year.

To pass the Microsoft SC-200 Exam, candidates must have a deep understanding of security operations concepts, tools, and techniques. They must also be able to analyze security data, identify threats, and respond to security incidents effectively. A strong knowledge of Microsoft security technologies, such as Azure Sentinel and Microsoft Defender for Endpoint, is also essential.

>> SC-200 Exam Questions <<

Valid SC-200 prep4sure vce & Microsoft SC-200 dumps pdf & SC-200 latest dumps

If you fail in the exam, we will refund you in full immediately at one time. After you buy our Microsoft Security Operations Analyst exam torrent you have little possibility to fail in exam because our passing rate is very high. But if you are unfortunate to fail in the exam we will refund you immediately in full and the process is very simple. If only you provide the scanning copy of the SC-200 failure marks we will refund you immediately. If you have any doubts about the refund or there are any problems happening in the process of refund you can contact us by mails or contact our online customer service personnel and we will reply and solve your doubts or questions timely.

Microsoft Security Operations Analyst Sample Questions (Q145-Q150):

NEW QUESTION # 145
You have a Microsoft Sentinel workspace named sws1.
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following

requirements:

* Minimize administrative effort.

* Use the principle of least privilege.

How should you configure the credentials? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure the connector to use:	A managed identity ▼
	A managed identity
	A service principal
	An Azure AD user account
Role to assign to the credentials:	Microsoft Sentinel Responder ▼
	Microsoft Sentinel Automation Contributor
	Microsoft Sentinel Reader
	Microsoft Sentinel Responder

Answer:

Explanation:

Answer Area

Configure the connector to use:	A managed identity ▼
	A managed identity
	A service principal
	An Azure AD user account
Role to assign to the credentials:	Microsoft Sentinel Responder ▼
	Microsoft Sentinel Automation Contributor
	Microsoft Sentinel Reader
	Microsoft Sentinel Responder

Explanation:

Answer Area

Configure the connector to use:	A managed identity ▼
Role to assign to the credentials:	Microsoft Sentinel Responder ▼

NEW QUESTION # 146

You have a Microsoft Sentinel workspace named Workspaces

You configure Workspace1 to c

ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.

You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.

How should you complete the query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

▼
_Im_Dns
Dns
imDns

▼
(starttime=ago(1d), responsecodename='NXDOMAIN')
| where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN"
| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)

Answer:

Explanation:

NEW QUESTION # 147
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
* Create and run playbooks
* Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. 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.
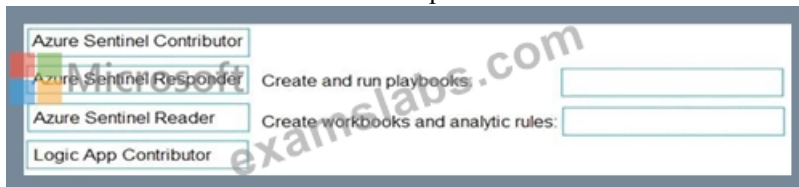
Answer:

Explanation:

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

NEW QUESTION # 148
You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps and has Cloud Discovery enabled.
You need to enrich the Cloud Discovery data. The solution must ensure that usernames in the Cloud Discovery traffic logs are associated with the user principal name (UPN) of the corresponding Microsoft Entra ID user accounts.
What should you do first?

- A. From Conditional Access App Control, configure User monitoring.
- B. Create a Microsoft 365 app connector.
- C. Create an Azure app connector.
- D. Enable automatic redirection to Microsoft 365 Defender.

Answer: B

Explanation:
In Microsoft Defender for Cloud Apps (MCAS), Cloud Discovery collects traffic logs to identify shadow IT usage and cloud app activities. To enrich this discovery data and map the usernames in traffic logs to actual Microsoft Entra ID (Azure AD) users, Defender for Cloud Apps must correlate the username with the user's User Principal Name (UPN).
According to Microsoft Defender for Cloud Apps documentation, this correlation happens automatically when you connect Microsoft 365 (formerly Office 365) through a Microsoft 365 app connector.
The connector integrates MCAS with Microsoft 365, allowing it to:
* Normalize usernames from discovery logs to match UPNs.
* Provide enriched identity details and activities across Microsoft 365 apps.
* Enable cross-app investigation, alert correlation, and conditional access governance.
Other options explained:
* Conditional Access App Control - Used for real-time session control, not Cloud Discovery enrichment.
* Enable automatic redirection to Microsoft 365 Defender - Used for portal integration, not data enrichment.
* Azure app connector - Used to connect third-party or Azure-hosted applications, not for UPN enrichment.
# Therefore, to enrich Cloud Discovery data with UPN mapping, you must create a Microsoft 365 app connector.

NEW QUESTION # 149
You need to create the test rule to meet the Azure Sentinel requirements.
What should you do when you create the rule?

- A. From Set rule logic, turn off suppression.
- B. From Set rule logic, map the entities.
- C. From Analytics rule details, configure the tactics.
- D. From Analytics rule details, configure the severity.

Answer: B

Explanation:
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

NEW QUESTION # 150
......

Success is has method. You can be successful as long as you make the right choices. ExamsLabs's Microsoft SC-200 exam training materials are tailored specifically for IT professionals. It can help you pass the exam successfully. If you're still catching your expertise to prepare for the exam, then you chose the wrong method. This is not only time-consuming and laborious, but also is likely to fail. But the remedy is not too late, go to buy ExamsLabs's Microsoft SC-200 Exam Training materials quickly. With it, you will get a different life. Remember, the fate is in your own hands.

- Real Microsoft SC-200 Dumps PDF Format 🔹 Download ✔ SC-200 🔹✔🔹 for free by simply entering ➡ www.easy4engine.com 🔹 website 🔹Cheap SC-200 Dumps
- Excellent 100% Free SC-200 – 100% Free Exam Questions | New SC-200 Dumps Questions 🔹 ☀ www.pdfvce.com 🔹☀🔹 is best website to obtain [SC-200] for free download 🔹Latest SC-200 Exam Testking
- SC-200 VCE Dumps 🔹 SC-200 Dump Check 🔹 SC-200 Reliable Exam Practice 🔹 Open website ➤ www.exam4labs.com 🔹 and search for ➡ SC-200 🔹 for free download 🔹Free SC-200 Sample
- Reliable SC-200 Exam Online 🔹 Exam Dumps SC-200 Collection 🔹 Valid Test SC-200 Tips 🔹 Search for { SC-200 } and download it for free immediately on ➤ www.pdfvce.com 🔹 🔹SC-200 Frequent Updates
- Latest SC-200 Exam Testking 🔹 Exam SC-200 Collection 🔹 SC-200 Reliable Exam Practice 🔹 Immediately open ➡ www.testkingpass.com 🔹🔹 and search for ⇒ SC-200 ⇐ to obtain a free download 🔹Exam Dumps SC-200 Collection
- knowyourmeme.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, 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.gpzj.net, 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

What's more, part of that ExamsLabs SC-200 dumps now are free: https://drive.google.com/open?id=1NiirUyVQ8QxJkuuPwnp7yaC9btZrNbYq