Learning SC-200 Mode | Latest SC-200 Exam Test

P.S. Free & New SC-200 dumps are available on Google Drive shared by BraindumpsIT: https://drive.google.com/open?id=1ydCF_6iW9r-FwYXb2NpNhE-jTxgzLRMU

The Microsoft SC-200 certification exam is most useful for candidates who are from the working class, but students who are still in school can also use Microsoft SC-200 dumps in place of searching for other exam-related literature. In order to put it simply, we can state that the Microsoft SC-200 Practice Questions are the only thing that can save you from failing the challenging SC-200 certification exam.

Microsoft SC-200 Exam is a popular certification among security professionals looking to advance their careers in the cybersecurity industry. It is a great way for professionals to demonstrate their expertise in security operations and incident response to potential employers. Microsoft Security Operations Analyst certification validates the candidate's ability to manage and respond to security incidents, and showcases their commitment to staying up-to-date with the latest security technologies and practices.

How to Register For Exam SC-200: Microsoft Security Operations Analyst?

Exam Register Link: https://examregistration.microsoft.com/?locale=en-us&examcode=SC-200&examname=Exam%20SC-200:%20Microsoft%20Security%20Operations%20Analyst&returnToLearningUrl=https%3A%2F%2Fdocs.microsoft.com%2Flearn%2Fcertifications%2Fexams%2Fsc-200

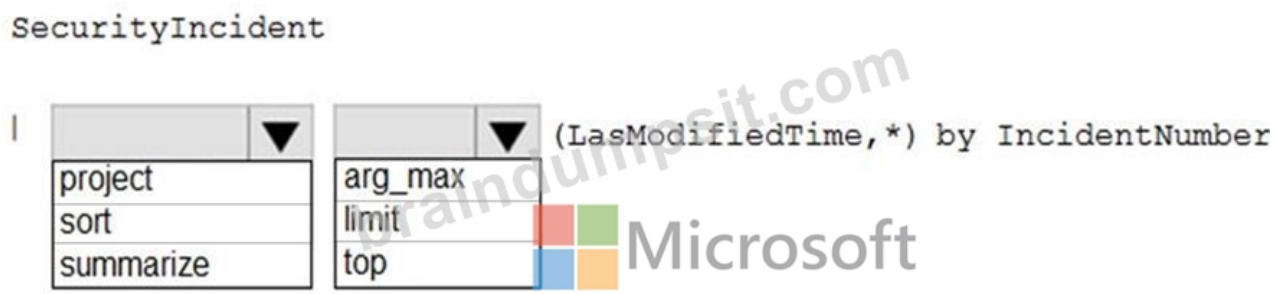
>> Learning SC-200 Mode <<

Latest Microsoft SC-200 Exam Test & SC-200 Valid Test Sims

There is no doubt that obtaining this SC-200 certification is recognition of their ability so that they can find a better job and gain the social status that they want. Most people are worried that it is not easy to obtain the certification of SC-200, so they dare not choose to start. We are willing to appease your troubles and comfort you. We are convinced that our SC-200 test material can help you solve your problems. Compared to other learning materials, our products are of higher quality and can give you access to the SC-200 certification that you have always dreamed of.

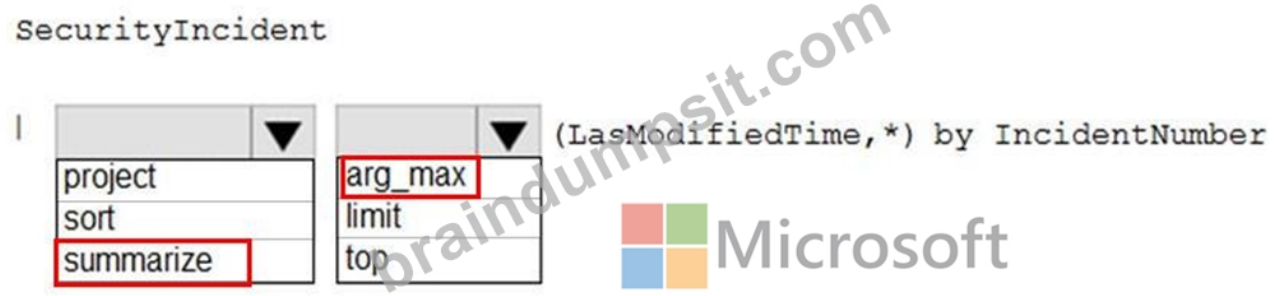
Microsoft Security Operations Analyst Sample Questions (Q267-Q272):

NEW QUESTION # 267
You need to create a query for a workbook. The query must meet the following requirements:
List all incidents by incident number.
Only include the most recent log for each incident.
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:



Reference:
https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

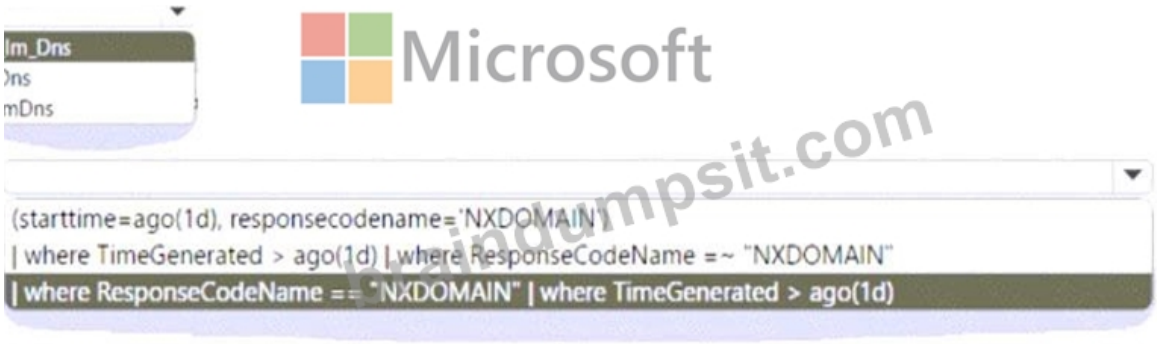
NEW QUESTION # 268
You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
A remediation action for an automated investigation quarantines a file across multiple devices.
You need to mark the file as safe and remove the file from quarantine on the devices.
What should you use in the Microsoft 365 Defender portal?

- A. From Threat tracker, review the queries.
- B. From Quarantine from the Review page, modify the rules.
- C. From the investigation page, review the AIR processes.
- D. From the History tab in the Action center, revert the actions.

Answer: D

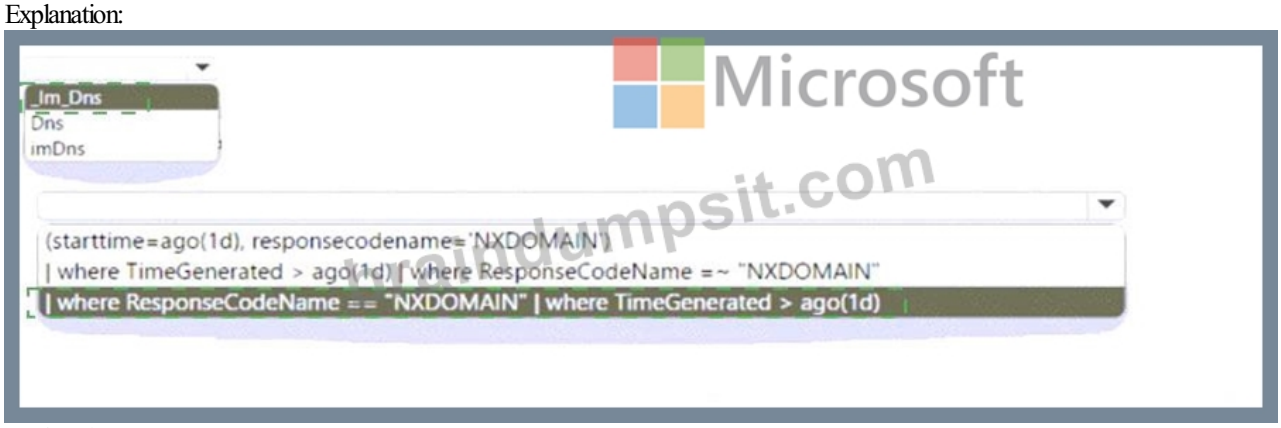
Explanation:
https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir- actions?view=o365-worldwide#undo-completed-actions

NEW QUESTION # 269
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.



Answer:

Explanation:



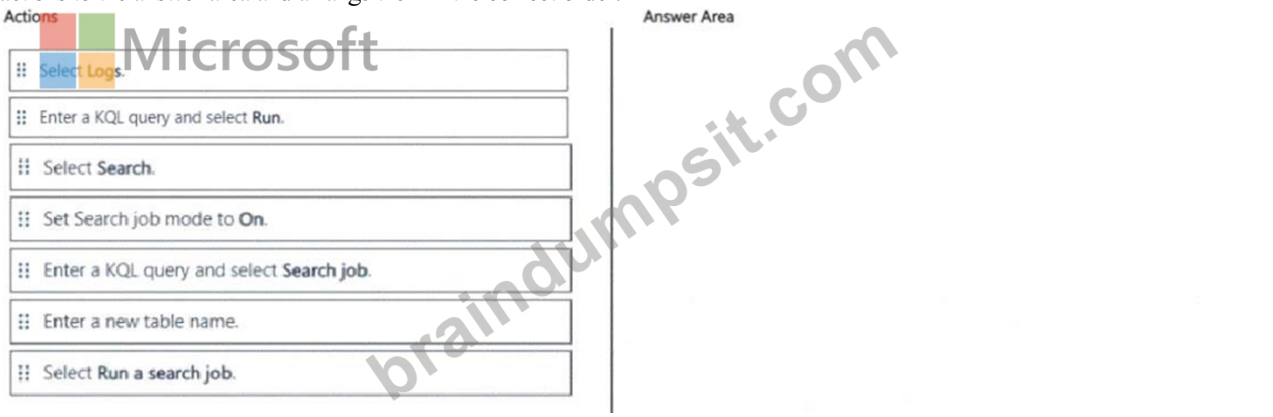
Explanation:

NEW QUESTION # 270

You have a Microsoft Sentinel workspace named Workspace1.

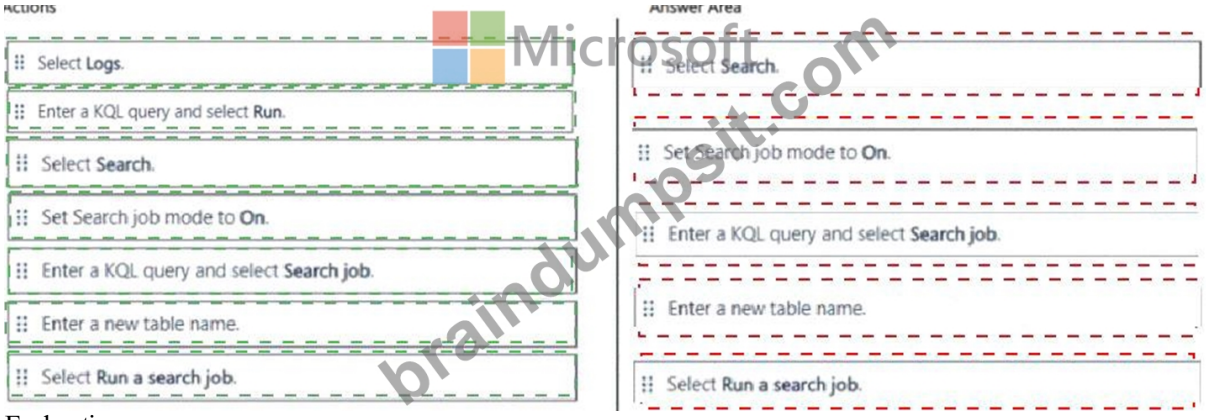
You need to run a KQL query as a search job.

Which five actions should you perform in Workspace 1 in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

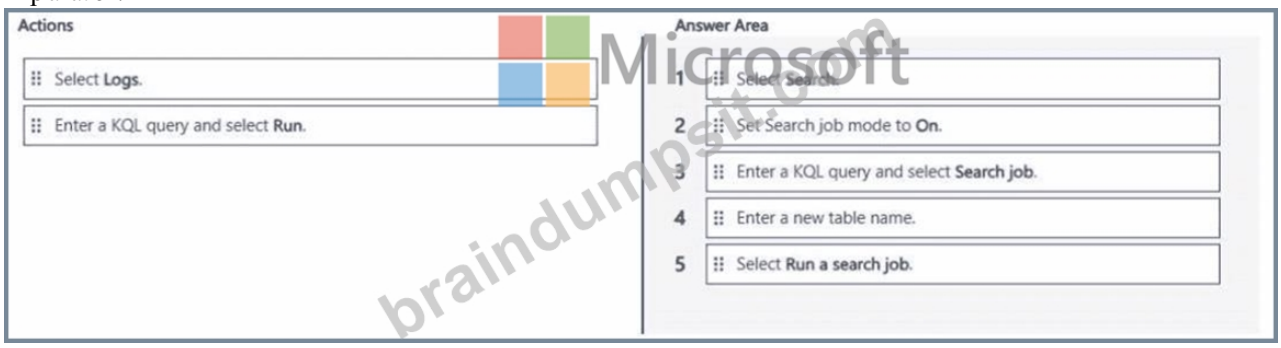


Answer:

Explanation:



Explanation:



NEW QUESTION # 271

You have an Azure subscription.

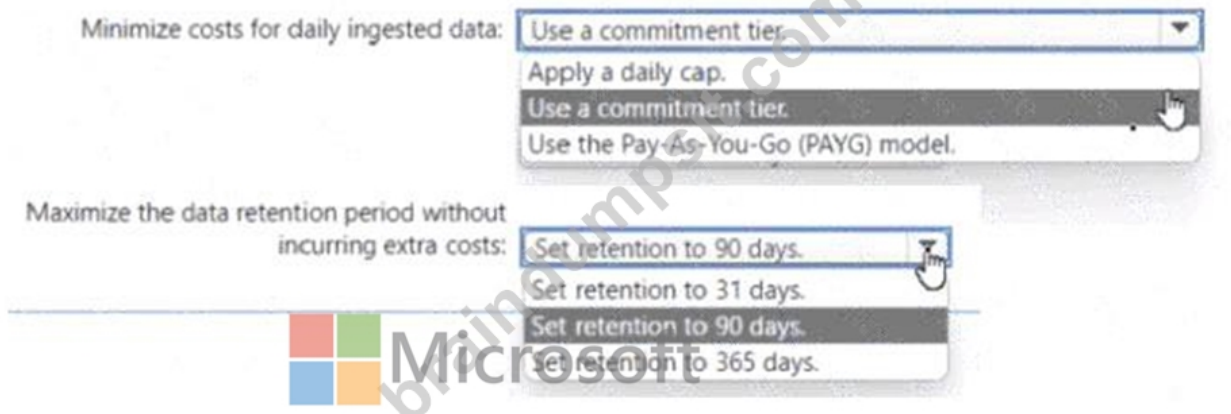
You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

* Minimize costs for daily ingested data.
* Maximize the data retention period without incurring extra costs.

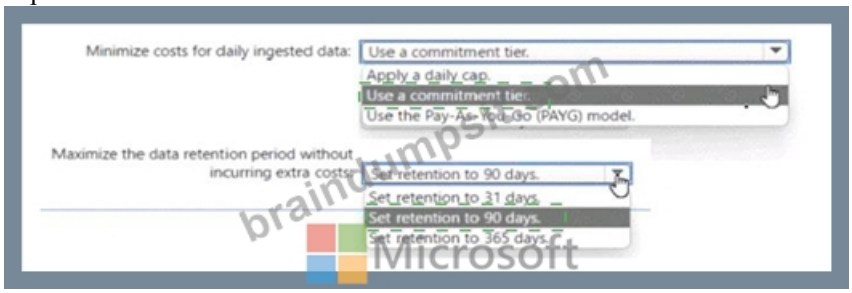
What should you do for each requirement? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.



Answer:

Explanation:



Explanation:

When designing a Microsoft Sentinel workspace, cost optimization and data retention management are two key considerations. Microsoft Sentinel stores data in an Azure Log Analytics workspace , and pricing for data ingestion and retention is managed through Log Analytics settings.

* Minimize costs for daily ingested data: Microsoft's documentation on Log Analytics pricing models states that you can choose between Pay-As-You-Go (PAYG) and Commitment Tiers . The Commitment Tier model allows you to commit to a fixed amount of da ily ingestion (for example, 20 GB/day in this case) at a lower per-GB cost compared to PAYG pricing. If your ingestion volume is predictable (as in this scenario-20 GB per day), this model provides significant cost savings without the administrative overhe ad of managing caps or throttling. Therefore, to minimize ingestion cost, the correct choice is "Use a commitment tier."

* Maximize the data retention period without incurring extra costs: By default, Microsoft Sentinel (via Log Analytics) provides 90 days o f data retention at no additional charge . Extending retention beyond 90 days incurs additional storage charges. According to Microsoft's official guidance, "Log Analytics retains data for 90 days at no cost; data kept beyond that period is billed at the re tention rate." Therefore, to maximize the free retention period while avoiding extra cost, the correct configuration is "Set retention to 90 days." Summary:

* Minimize costs for daily ingested data # Use a commitment tier
* Maximize retention without extra cos ts # Set retention to 90 days

This configuration ensures both cost efficiency and maximum free data availability, aligning with Microsoft Security Operations (SecOps) and Sentinel best practices.

NEW QUESTION # 272

.....

P.S. Free & New SC-200 dumps are available on Google Drive shared by BraindumpsIT: https://drive.google.com/open?id=1ydCF_6iW9r-FwYXb2NpNhE-jTxgzLRMU