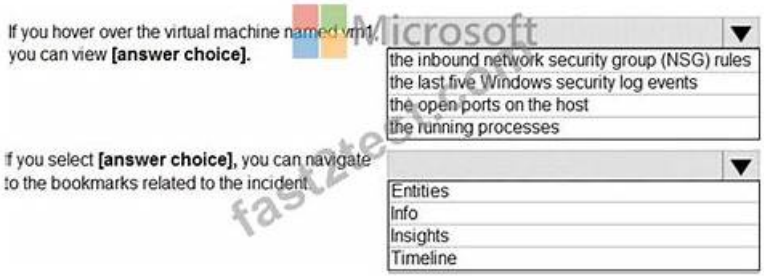
Guaranteed Success with Real and Updated Microsoft SC-200 Exam Questions



P.S. Free & New SC-200 dumps are available on Google Drive shared by TestValid: https://drive.google.com/open?id=1pv7psc3oEAyugqWg0fPGfjRipwzcMCFn

Many people prefer to buy our SC-200 valid study guide materials because they deeply believe that if only they buy them can definitely pass the SC-200 test. The reason why they like our SC-200 guide questions is that our study materials' quality is very high and the service is wonderful. For years we always devote ourselves to perfecting our SC-200 Study Materials and shaping our products into the model products which other companies strive hard to emulate. We boost the leading research team and the top-ranking sale service.

Microsoft SC-200 exam, also known as the Microsoft Security Operations Analyst exam, is a highly sought-after certification for professionals working in the field of cybersecurity. SC-200 Exam is designed to test the candidate's knowledge and skills in threat detection, incident response, and compliance management.

>> SC-200 Free Test Questions <<

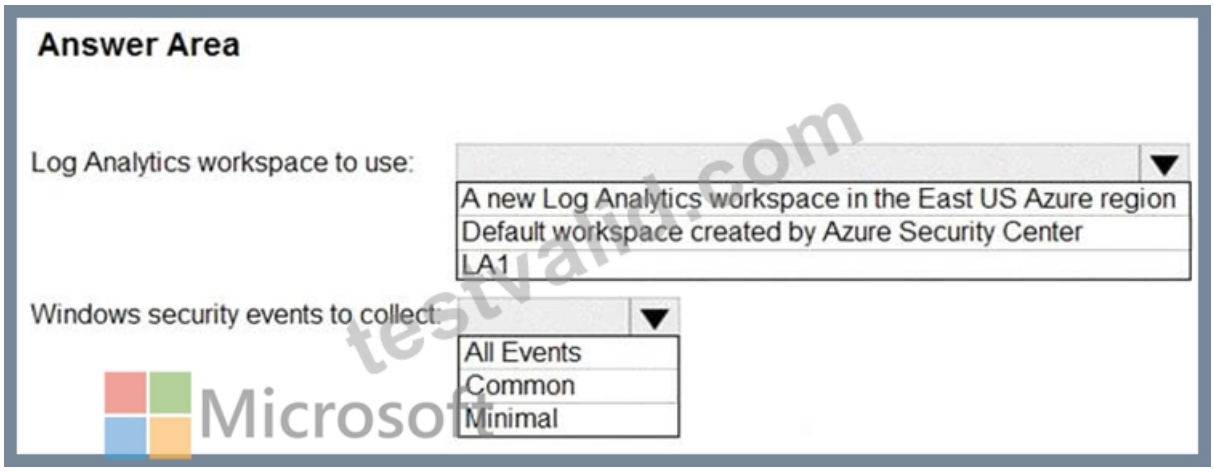
SC-200 Dumps PDF Format Practice Test

During nearly ten years, our SC-200 exam questions have met with warm reception and quick sale in the international market. Our SC-200 study materials are not only as reasonable priced as other makers, but also they are distinctly superior in the many respects. With tens of thousands of our loyal customers supporting us all the way, we believe we will do a better job in this career. More and more candidates will be benefited from our excellent SC-200 training guide!

Microsoft Security Operations Analyst (SC-200) certification exam is designed to test the skills and knowledge of security professionals who are responsible for detecting, investigating, and responding to security incidents in a Microsoft environment. SC-200 Exam is ideal for individuals who have experience working with Microsoft security technologies and are looking to advance their careers in the field of cybersecurity.

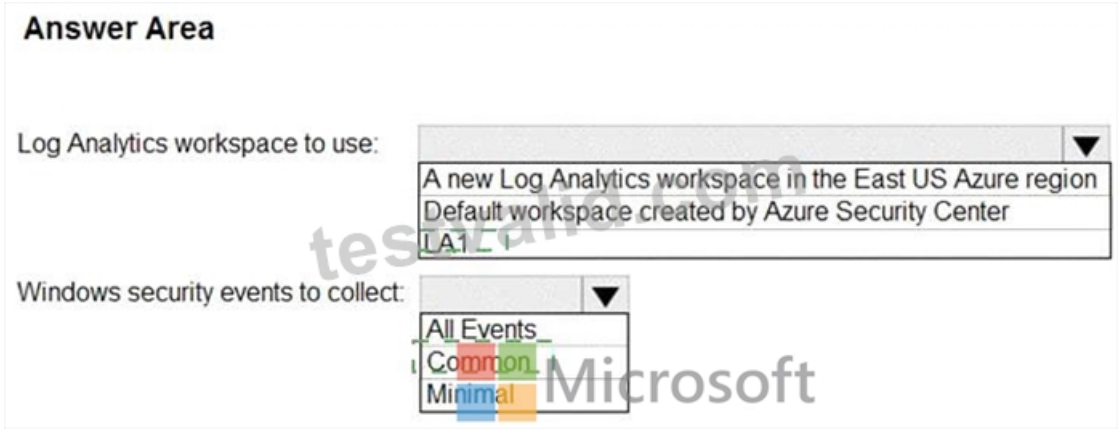
Microsoft Security Operations Analyst Sample Questions (Q96-Q101):

NEW QUESTION # 96
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 # 97
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to configure Defender for Cloud to mitigate the following risks:
* Vulnerabilities within the application source code
* Exploitation toolkits in declarative templates
* Operations from malicious IP addresses
* Exposed secrets
Which two Defender for Cloud services should you use? Each correct answer presents part of the solution.
NOTE: Each correct answer is worth one point.

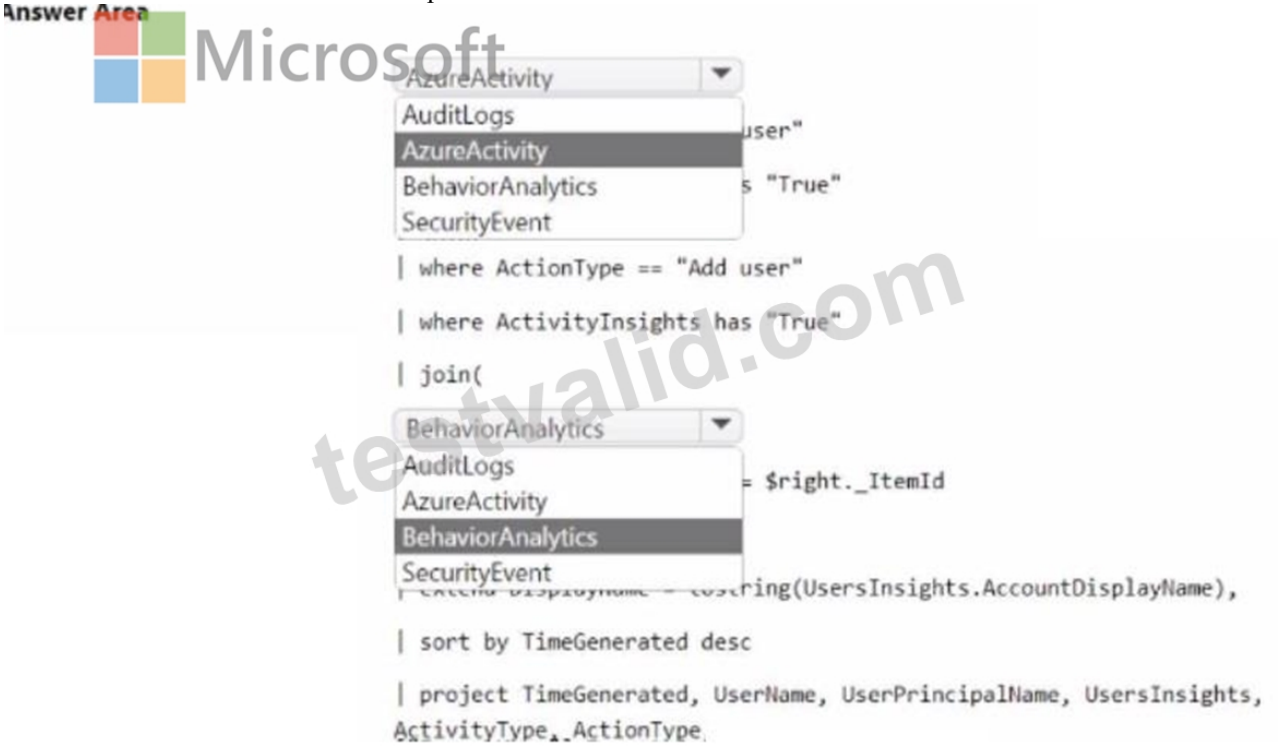
- A. Microsoft Defender for App Service
- B. Microsoft Defender for DevOps
- C. Microsoft Defender for APIs
- D. Microsoft Defender for Resource Manager
- E. Microsoft Defender for Servers

Answer: B,D

Explanation:

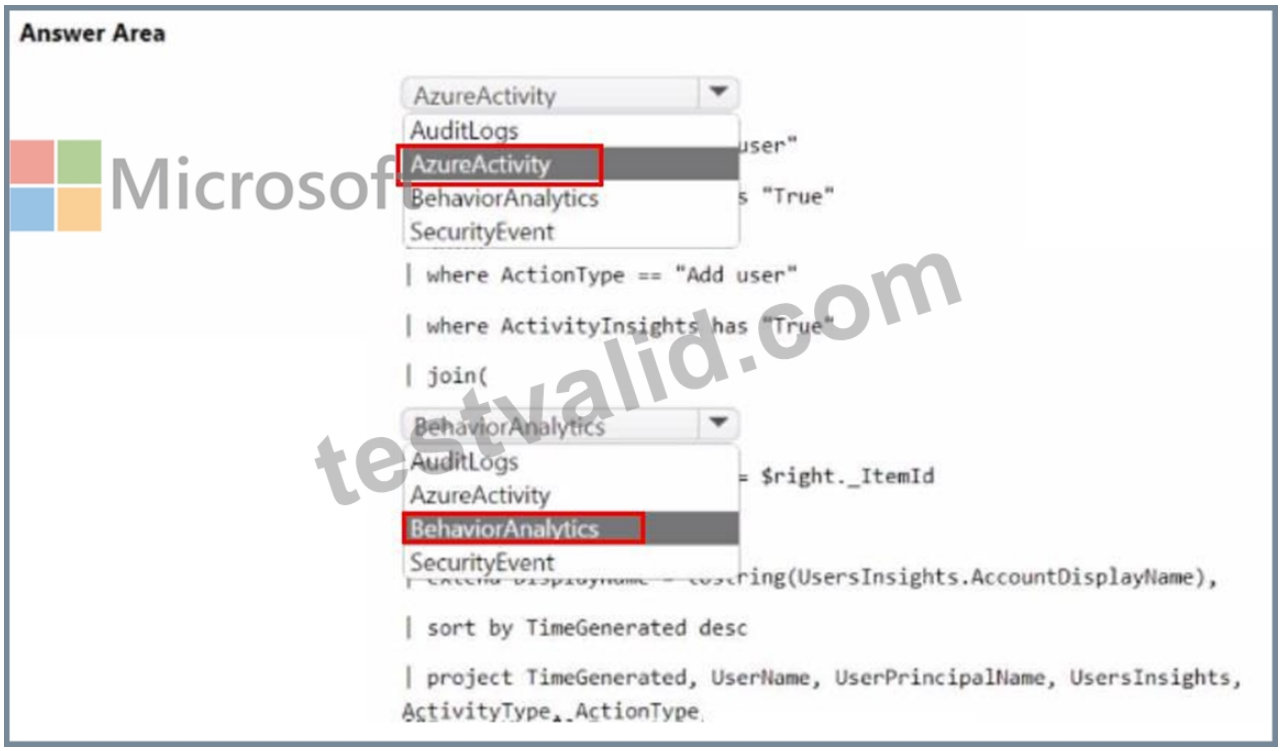
Microsoft Defender for Cloud provides multiple specialized Defender plans to protect different layers of your environment.
* Microsoft Defender for DevOps helps identify vulnerabilities in source code, exposed secrets, and insecure dependencies by integrating with CI/CD systems like GitHub and Azure DevOps. It scans repositories for known vulnerabilities (CVEs), weak configurations, and exposed credentials before code is deployed. This directly addresses the risks:
* Vulnerabilities within application source code
* Exposed secrets
* Microsoft Defender for Resource Manager protects the Azure control plane and monitors management operations to detect threats such as deployment of malicious templates, exploitation toolkits in IaC (Infrastructure as Code), and operations from malicious IP addresses. It provides alerts when suspicious control-plane actions occur, for example, unexpected activity via ARM or Terraform. This covers:
* Exploitation toolkits in declarative templates
* Operations from malicious IP addresses
Together, these two Defender plans (Defender for DevOps + Defender for Resource Manager) mitigate all four risks listed in the question.
Correct answers: B. Microsoft Defender for Resource Manager and D. Microsoft Defender for DevOps

NEW QUESTION # 98
You have a Microsoft Sentinel workspace named sws1.
You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.
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 Area



Answer:

Explanation:



NEW QUESTION # 99
You have a Microsoft Sentinel workspace named SW1.
In SW1. you enable User and Entity Behavior Analytics (UEBA).
You need to use KQL to perform the following tasks:
* View the entity data that has fields for each type of entity.
* Assess the quality of rules by analyzing how well a rule performs.
Which table should you use in KQL for each task? To answer, drag the appropriate tables to the correct tasks.
Each table 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:

When User and Entity Behavior Analytics (UEBA) is enabled in Microsoft Sentinel, it creates several dedicated tables within the Log Analytics workspace to store processed data for behavioral analytics and anomaly detection. Each table serves a specific purpose according to Microsoft documentation.

* BehaviorAnalytics Table - for viewing entity dataThe BehaviorAnalytics table stores enriched information about entities (such as users, hosts, IP addresses, and applications) and their observed behaviors. Each record includes multiple fields that describe user or entity activities, risk scores, and behavioral baselines. Microsoft Sentinel documentation states:

"Use the BehaviorAnalytics table to view the entity data collected and analyzed by UEBA. This table contains fields for each type of entity, including account, host, and IP data." Therefore, to view the entity data with detailed attributes for each type, you query the BehaviorAnalytics table in KQL.

* Anomalies Table - for assessing rule qualityThe Anomalies table is used to analyze the results of anomaly detection rules and evaluate their effectiveness. Each record represents an anomaly event generated by UEBA's machine learning or statistical models. Microsoft's UEBA and Sentinel analytics documentation explains:

"Use the Anomalies table to assess the performance and quality of your anomaly detection rules. The table helps you identify how well each rule detects unusual activities and whether it produces false positives." Thus, when you need to measure how well your rules perform (i.e., their quality, hit rate, or alert effectiveness), you use the Anomalies table.

Summary Mapping:

* View entity data # BehaviorAnalytics
* Assess rule quality # Anomalies

This mapping aligns directly with the functionality of UEBA-related tables in Microsoft Sentinel and follows official documentation for analyzing entity behaviors and anomaly rule performance.

NEW QUESTION # 100

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

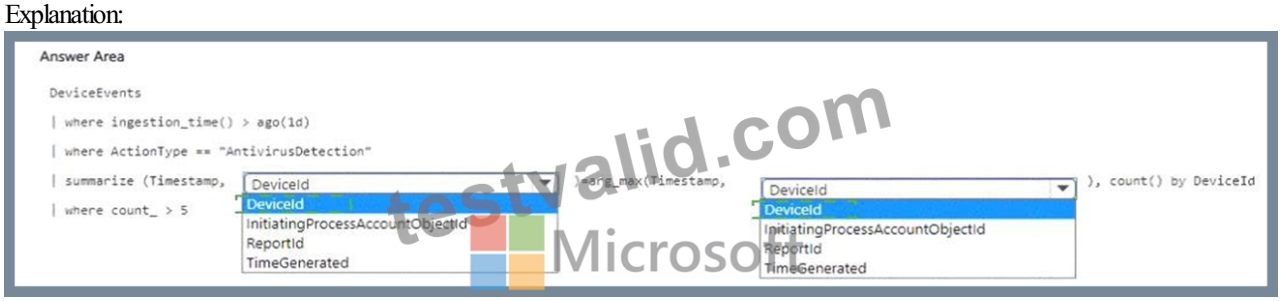
You need to create a custom detection rule that will identify devices that had more than five antivirus detections within the last 24 hours.

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 # 101

.....

Exam SC-200 Study Solutions: https://www.testvalid.com/SC-200-exam-collection.html

- Quiz 2025 Pass-Sure Microsoft SC-200 Free Test Questions □ Go to website ⇛ www.torrentvce.com ⇚ open and search for □ SC-200 □ to download for free □Online SC-200 Version
- Get Help From Top Notch Pdfvce SC-200 Exam Practice Questions □ Search for □ SC-200 □ and download it for free immediately on 【 www.pdfvce.com 】 □SC-200 Test Sample Questions
- SC-200 Test Sample Questions □ SC-200 Reliable Test Forum □ SC-200 Updated CBT □ Search for [SC-200] and easily obtain a free download on ▸ www.testkingpdf.com ◂ □SC-200 Exam Dumps Collection
- TOP SC-200 Free Test Questions: Microsoft Security Operations Analyst - High Pass-Rate Microsoft Exam SC-200 Study Solutions □ Search for □ SC-200 □ and easily obtain a free download on [www.pdfvce.com] □SC-200 Valid Test Notes
- Get Help From Top Notch www.dumps4pdf.com SC-200 Exam Practice Questions □ Copy URL ➡ www.dumps4pdf.com □□□ open and search for 【 SC-200 】 to download for free □Exam SC-200 Simulations
- Free PDF Quiz 2025 Microsoft Perfect SC-200 Free Test Questions □ Simply search for 《 SC-200 》 for free download on 【 www.pdfvce.com 】 □Formal SC-200 Test
- Quiz 2025 Pass-Sure Microsoft SC-200 Free Test Questions ✍ ➠ www.prep4sures.top □ is best website to obtain ➽ SC-200 □ for free download □SC-200 Pass Exam
- SC-200 Exam Syllabus □ SC-200 Test Sample Questions □ SC-200 Test Braindumps □ Search for □ SC-200 □ and download it for free immediately on ▸ www.pdfvce.com ◂ □SC-200 Reliable Guide Files
- Quiz 2025 Pass-Sure Microsoft SC-200 Free Test Questions □ Search for ☀ SC-200 □☀□ and easily obtain a free download on ➥ www.exam4pdf.com □ □Exam SC-200 Simulations
- Top SC-200 Free Test Questions | High-quality Microsoft Exam SC-200 Study Solutions: Microsoft Security Operations Analyst □ Download ✔ SC-200 □✔□ for free by simply searching on 《 www.pdfvce.com 》 □New SC-200 Dumps
- Free PDF Quiz 2025 Microsoft Updated SC-200 Free Test Questions □ Search for ➥ SC-200 □ and download it for free on 「 www.prep4pass.com 」 website □Formal SC-200 Test
- www.stes.tyc.edu.tw, sdmartlife.com, zeritenetwork.com, www.hsw021.com, wheelwell.efundisha.co.za, www.stes.tyc.edu.tw, mylearningstudio.site, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, test.york360.ca, Disposable vapes

DOWNLOAD the newest TestValid SC-200 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1pv7psc3oEAyugqWg0fPGfjRipwzcMCFn