SC-200 Test Testking, Exam SC-200 Study Guide

Microsoft Security Operations Analyst (SC-200) Exam
Learning path
Start Here
Detect, investigate, respond, and remediate identity threats
Design and configure a Microsoft Defender for Cloud implementation
Configure Security Orchestration Automation and Response (SOAR) in the Microsoft Sentinel
Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365
Microsoft CERTIFIED
SECURITY OPERATIONS ANALYST
ASSOCIATE
SC-200
WHIZLABS

DOWNLOAD the newest TestkingPDF SC-200 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1WhLbFGEbCovZB6h7OCnCbv6cb5qP0nXD

With the intense competition in labor market, it has become a trend that a lot of people, including many students, workers and so on, are trying their best to get a SC-200 certification in a short time. The SC-200 exam prep is produced by our expert, is very useful to help customers pass their exams and get the certificates in a short time. We are going to show our SC-200 Guide braindumps to you. We can sure that our product will help you get the certificate easily. If you are wailing to believe us and try to learn our SC-200 exam torrent, you will get an unexpected result.

Microsoft SC-200 certification exam is an important credential for security professionals who work with Microsoft products and services. Passing the exam demonstrates that the candidate has the knowledge and skills required to protect Microsoft environments from cyber threats. To prepare for the exam, candidates should have experience in security operations and be familiar with Microsoft 365 Defender, Azure Defender, and Azure Sentinel. Microsoft offers several resources to help candidates prepare for the exam, and passing the exam earns the candidate the Microsoft Security Operations Analyst certification.

Microsoft SC-200 Certification Exam is a valuable asset for anyone who wants to pursue a career in cybersecurity. It is an excellent way to demonstrate one's knowledge and skills in security operations analysis and showcase their commitment to professional development. Microsoft Security Operations Analyst certification is recognized globally and can help candidates stand out in a competitive job market.

>> SC-200 Test Testking <<

Exam SC-200 Study Guide | Dumps SC-200 Discount

Today, the IT industry is facing fierce competition, you will feel powerless, this is inevitable. All you have to do is to escort your career. Of course, you have many choices. I recommend that you use the TestkingPDF Microsoft SC-200 Exam Questions And Answers, it is a good helper to help your success of IT certification. So what you still waiting for, go to get new TestkingPDF Microsoft SC-200 exam training materials early.

Microsoft SC-200 certification is highly valued in the industry as it validates the skills and knowledge required to secure Microsoft environments effectively. It provides an opportunity for security professionals to demonstrate their expertise and stand out in the job market. Additionally, the certification can help professionals advance their careers and earn higher salaries. Overall, the Microsoft SC-200 Certification is an excellent investment for security professionals who want to enhance their skills and knowledge in Microsoft security technologies.

Microsoft Security Operations Analyst Sample Questions (Q157-Q162):

NEW QUESTION # 157
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a user named User1.
You need to ensure that User1 can manage Microsoft Defender XDR custom detection rules and Endpoint security policies. The solution must follow the principle of least privilege.
Which role should you assign to User1?

- A. Security Operator
- B. Desktop Analytics Administrator

- C. Security Administrator
- D. Cloud Device Administrator

Answer: C

Explanation:
In Microsoft 365 E5 environments that use Microsoft Defender XDR, role-based access control (RBAC) is enforced across the Microsoft Defender portal to align with least-privilege principles. To manage custom detection rules (such as scheduled analytics rules in Defender XDR) and endpoint security policies (such as antivirus, firewall, or attack surface reduction policies in Microsoft Defender for Endpoint), the required role is Security Administrator.
According to Microsoft documentation, the Security Administrator role:
* "Can manage security settings in Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps."
* "Has full permissions to create, edit, and delete security policies, alerts, and detections."
* "Can configure and manage custom detection rules, automated investigation settings, and advanced hunting queries." By contrast:
* Security Operator can view alerts and incidents and take limited response actions but cannot create or manage detection rules or policies.
* Desktop Analytics Administrator relates to Windows analytics and endpoint readiness reporting, not Defender XDR management.
* Cloud Device Administrator primarily manages device onboarding and enrollment in Microsoft Intune or Azure AD, not Defender policies or detections.
Following the principle of least privilege, Security Administrator grants exactly the rights needed to manage Defender XDR custom detection rules and endpoint security policies-without assigning excessive administrative permissions across the tenant.
Therefore, the correct and verified answer is C. Security Administrator.

NEW QUESTION # 158
You have an Azure subscription named Sub1 and an Azure DevOps organization named AzDO1. AzDO1 uses Defender for Cloud and contains a project that has a YAML pipeline named Pipeline1.
Pipeline1 outputs the details of discovered open source software vulnerabilities to Defender for Cloud.
You need to configure Pipeline1 to output the results of secret scanning to Defender for Cloud, What should you add to Pipeline1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

NEW QUESTION # 159
You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs to a syslog server. The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point

Answer:

Explanation:

Explanation:

NEW QUESTION # 160
You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

In Microsoft Sentinel's Advanced Security Information Model (ASIM), DNS queries are normalized through the Im_Dns parser, which unifies DNS telemetry from multiple sources (Infoblox, Windows DNS, Azure Firewall DNS proxy, etc.). Microsoft guidance states that when you need broad compatibility and want to "use built-in ASIM parsers whenever possible," you should call the generic Im_Dns() parser. To minimize overhead, ASIM provides a pack parameter that restricts the parser to a specific content pack (vendor/source) so it won't iterate through all available source parsers under the hood. For Infoblox NIOS, you pass the Infoblox pack via the pack parameter, which limits parsing to the Infoblox implementation and reduces query cost/latency while keeping the query portable across environments.

Putting it together, the recommended pattern is:

```
Im_Dns(pack="InfobloxNIOS")
| where DnsResponseCodeName == "NXDOMAIN"
| summarize count()
```

This approach satisfies all requirements:

* Uses built-in ASIM (Im_Dns).
* Minimizes query overhead (uses pack to limit parsing to Infoblox).
* Targets NXDOMAIN responses for counting DNS request failures from Infoblox1.

NEW QUESTION # 161

You have a Microsoft 365 B5 subscription that uses Microsoft Defender XDR. You are investigating an incident You need to review the incident tasks that were performed. What can you use on the Incident page?

- A. Tasks, Activity log, and Alert timeline
- B. Tasks and Alert timeline only
- C. Tasks and Activity log only
- D. Tasks only

Answer: A

Explanation:

On the Microsoft Defender (Microsoft 365 Defender) Incident page, investigators need a complete view of what actions were taken and when. The UI provides multiple panes to support that: the Tasks area (lists manual and automated investigation/remediation tasks assigned to the incident), the Activity log (chronological audit of user and system actions taken on the incident such as assignments, status changes, playbook runs and remediation actions), and the Alert timeline (a timeline view showing the alerts that make up the incident and the sequence of alerts and related detections/events). Microsoft's investigation guidance describes all three surfaces as part of the incident investigation workflow: tasks capture work items and owner actions, the activity log provides an auditable history of actions and changes, and the alert timeline visualizes the alert and event sequence that drove the incident.

Because the question asks specifically for reviewing the incident tasks that were performed, the incident page exposes the tasks list and also the activity log and alert timeline so you can see when tasks ran, who ran them, what automated playbooks or remediation executed, and how those tasks related to the underlying alerts. For full incident forensics and auditability you use Tasks + Activity log + Alert timeline.

NEW QUESTION # 162

......

200 ◀ and easily obtain a free download on [www.pdfvce.com] □New SC-200 Mock Test

- 2026 RealisticExam SC-200 Study Guide - Microsoft Microsoft Security Operations Analyst Test Testking 100% Pass □ Search for （ SC-200 ） and download it for free immediately on ➽ www.pdfdumps.com □ □SC-200 Well Prep
- Pass Guaranteed Quiz 2026 Microsoft Authoritative SC-200 Test Testking □ Search for □ SC-200 □ and download it for free on “ www.pdfvce.com ” website □SC-200 Well Prep
- Pass Guaranteed 2026 Microsoft Professional SC-200: Microsoft Security Operations Analyst Test Testking □ ▶ www.testkingpass.com ◀ is best website to obtain 《 SC-200 》 for free download ◀SC-200 Latest Practice Materials
- Latest SC-200 Test Camp □ SC-200 Well Prep □ SC-200 Latest Exam Discount □ Download ✔ SC-200 □✔□ for free by simply entering { www.pdfvce.com } website □Reliable SC-200 Exam Simulator
- Enhance Your Confidence with the Online Microsoft SC-200 Practice Test Engine □ Search on ▷ www.torrentvce.com ◁ for ▷ SC-200 ◁ to obtain exam materials for free download □Exam SC-200 Experience
- 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, 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, www.stes.tyc.edu.tw, stanchionacademy.com, 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 TestkingPDF: https://drive.google.com/open?id=1WhLbFGEbCovZB6h7OCnCbv6cb5qP0nXD