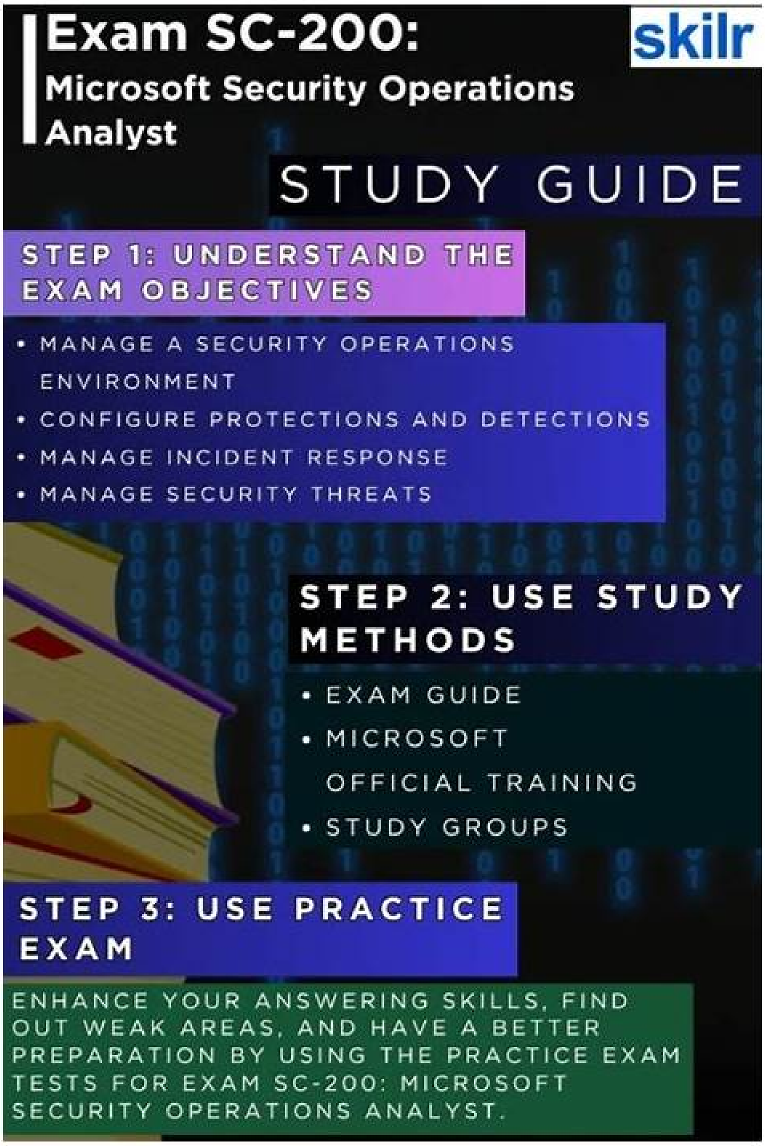
Microsoft SC-200 Valid Exam Guide & Brain Dump SC-200 Free



Exam SC-200:
Microsoft Security Operations Analyst

skilr

STUDY GUIDE

STEP 1: UNDERSTAND THE EXAM OBJECTIVES

- MANAGE A SECURITY OPERATIONS ENVIRONMENT
- CONFIGURE PROTECTIONS AND DETECTIONS
- MANAGE INCIDENT RESPONSE
- MANAGE SECURITY THREATS

STEP 2: USE STUDY METHODS

- EXAM GUIDE
- MICROSOFT OFFICIAL TRAINING
- STUDY GROUPS

STEP 3: USE PRACTICE EXAM

ENHANCE YOUR ANSWERING SKILLS, FIND OUT WEAK AREAS, AND HAVE A BETTER PREPARATION BY USING THE PRACTICE EXAM TESTS FOR EXAM SC-200: MICROSOFT SECURITY OPERATIONS ANALYST.

BONUS!!! Download part of ExamBoosts SC-200 dumps for free: https://drive.google.com/open?id=1AauaZi3-IY-MGY7Iefn62K6sMYtVGBFS

Every user has rated study material positively and passed the SC-200 Exam. ExamBoosts gives a guarantee to the customers that if they fail to pass the Microsoft Security Operations Analyst (SC-200) certification on the very first try despite all their efforts they can claim their money back according to terms and conditions. A team of experts is working day and night in order to make the product successful day by day and provide the customers with the best experience.

Microsoft SC-200 Certification Exam is an advanced-level certification that validates the skills and knowledge of security professionals in using Microsoft security technologies to protect against cyber threats. It covers topics such as threat intelligence, incident response, security operations automation, and governance, risk, and compliance (GRC). By passing this certification exam, candidates demonstrate their ability to use Microsoft security solutions to identify, investigate, and respond to security incidents.

>> Microsoft SC-200 Valid Exam Guide <<

Newest SC-200 Valid Exam Guide | Amazing Pass Rate For SC-200 Exam |

Well-Prepared SC-200: Microsoft Security Operations Analyst

We know that the standard for most workers become higher and higher; so we also set higher goal on our SC-200 guide questions. Our training materials put customers' interests in front of other points, committing us to the advanced SC-200 learning materials all along. Until now, we have simplified the most complicated SC-200 Guide questions and designed a straightforward operation system, with the natural and seamless user interfaces of SC-200 exam question grown to be more fluent, we assure that our practice materials provide you a total ease of use.

What is the format of Microsoft SC-200 Exam

- Exam Duration: 130 minutes
- Exam Format: Multiple choice questions
- Exam Length: 40 questions
- Passing score: 70%
- Language: English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Russian, Arabic (Saudi Arabia), Chinese (Traditional), Italian

Microsoft SC-200 (Microsoft Security Operations Analyst) Certification Exam is a highly sought-after certification in the field of cybersecurity. Microsoft Security Operations Analyst certification is designed for security professionals who are responsible for monitoring and responding to security threats in Microsoft environments. The SC-200 Exam is focused on testing the skills and knowledge of security operations analysts who work with Microsoft 365 Defender, Azure Defender, and other Microsoft security products.

Microsoft Security Operations Analyst Sample Questions (Q204-Q209):

NEW QUESTION # 204
You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event.
You create the following rule query.
By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. resource group
- B. user
- C. computer
- D. IP address

Answer: B,C

NEW QUESTION # 205
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You are implementing a deception rule.
You need to provide a custom lure file.
For the custom lure, you set Planting path to HOME.
Which types of files can you use for the custom lure, and in which home directory should the file be located on a device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:
Question Part 1: Which types of files can you use for the custom lure?
Q1 Answer:
EXE, XLSX, and PDF
According to your screenshot (File types drop-down), you can use the following file types for a custom lure in Microsoft Defender

XDR deception rules:
* EXE
* XLSX
* PDF
You can select any combination of these, so EXE, XLSX, and PDF are all supported as custom lure file types.
Question Part 2: In which home directory should the file be located on a device?
Q2 Answer:
The Active Directory user
When you set the Planting path to HOME in a deception rule, the file should be planted in the home directory of a user. According to the available drop-down options and Microsoft documentation, the typical recommended choice for corporate environments (and specifically for most deception scenarios) is "The Active Directory user". This ensures the lure is placed where the intended target (a domain user) is likely to encounter it.

NEW QUESTION # 206
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
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
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=

NEW QUESTION # 207
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.
Does this meet the goal?

- A. No
- B. Yes

Answer: A

Explanation:
Section: [none]
Explanation:
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

NEW QUESTION # 208
You have an Azure subscription that contains a guest user named User1 and a Microsoft Sentinel workspace named workspace1.
You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. The solution must use the principle of least

privilege.
Which roles should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
□

Answer:

Explanation:
□
Explanation:
□
In Microsoft Sentinel, incident management and investigation permissions are controlled through Sentinel- specific Azure roles. To allow a user (including a guest user) to triage incidents - meaning they can view, assign, and update incident statuses, but not modify analytics rules or automation logic - the correct Azure role is Microsoft Sentinel Responder.
Here's the breakdown:
1## Azure role # Microsoft Sentinel Responder
* The Sentinel Responder role grants permissions to view incidents, update incident status, assign incidents, and run playbooks on incidents.
* It follows the principle of least privilege by limiting access to only incident response and not allowing rule creation, workbook management, or data connector configuration.
* The Sentinel Contributor role, on the other hand, provides broader permissions (including modifying analytic rules), which exceeds the requirement of "triaging incidents."
* Therefore, Microsoft Sentinel Responder is the correct and least-privilege Azure role.
2## Azure AD role # Directory readers
* To investigate and triage incidents effectively, Sentinel users must be able to resolve user identities (such as usernames, group membership, and object IDs) within Microsoft Entra ID (Azure AD).
* The Directory Readers role provides read-only access to directory data, allowing the user to view identities but not modify them.
* This minimal permission satisfies Sentinel's identity lookup needs without elevating the user to a global administrative or global reader role.
# Final Answers:
* Azure role: Microsoft Sentinel Responder
* Azure AD role: Directory readers

NEW QUESTION # 209
......

www.stes.tyc.edu.tw, wjhsd.instructure.com, zenwriting.net, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that ExamBoosts SC-200 dumps now are free: https://drive.google.com/open?id=1AauaZi3-IY-MGY7Iefn62K6sMYtVGBFS