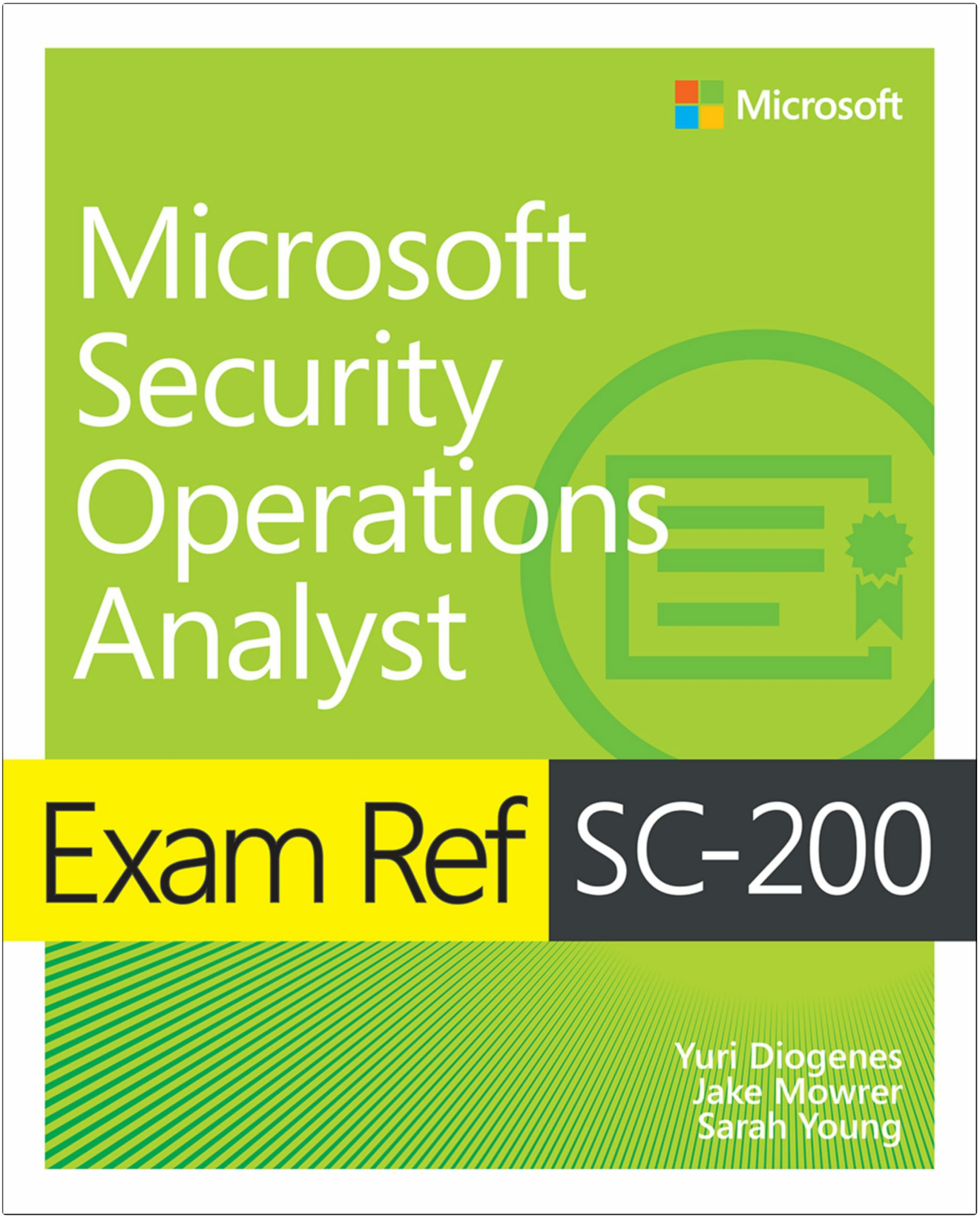
Microsoft Press SC-200

Exam Ref SC-200 Microsoft Security Operations Analyst

Official Study Guide for Microsoft Certification Exam SC-200

Introduction

This manual serves as a comprehensive guide for individuals preparing for Microsoft Exam SC-200, focusing on the skills and knowledge required to secure IT systems and rapidly remediate active attacks. It is designed for Windows administrators and emphasizes critical thinking and decision-making acumen essential for success at the Microsoft Certified Associate level.



The book cover features the title 'Microsoft Security Operations Analyst' prominently in white text on a bright green background. Below this, a yellow bar contains 'Exam Ref' in black text, followed by 'SC-200' in white text on a dark grey background. The Microsoft logo is in the top right corner. At the bottom right, the authors' names, Yuri Diogenes, Jake Mowrer, and Sarah Young, are listed.

Setup and Prerequisites

Before beginning your study with this Exam Ref, it is assumed that you possess foundational experience with threat

management, monitoring, and/or response within Microsoft 365 environments. This prior knowledge will enable you to fully leverage the advanced concepts and scenarios presented in the book.

To maximize your learning experience, ensure you have access to a computer with internet connectivity to explore referenced Microsoft documentation and online resources.

Operating and Study Methodology

This Exam Ref is structured to align directly with the official exam objectives for SC-200. To effectively use this book, focus on understanding the core concepts and applying them through the strategic, what-if scenarios provided.

Key Exam Objectives Covered:

- **Mitigate threats using Microsoft 365 Defender:** Learn to detect, investigate, respond, and remediate threats across productivity, endpoints, identity, and applications within the Microsoft 365 ecosystem.
- **Mitigate threats using Microsoft Defender for Cloud:** Understand how to design and configure Azure Defender implementations, plan and use data connectors to ingest data sources, and manage alert rules.
- **Mitigate threats using Microsoft Sentinel:** Explore designing and configuring Azure Sentinel workspaces, managing rules and incidents, configuring SOAR (Security Orchestration, Automation, and Response), using workbooks for data analysis, and threat hunting.

Each section of the book is designed to build your expertise progressively. Pay close attention to the practical examples and case studies, as they are crucial for developing the decision-making skills tested in the exam.

Regularly review the objectives and test your understanding with practice questions, if available, to solidify your knowledge.

Maintaining Knowledge and Updates

The field of cybersecurity and Microsoft technologies evolves rapidly. To ensure your knowledge remains current, it is recommended to:

- Regularly visit the official Microsoft Learn platform for updates related to the SC-200 exam objectives and associated technologies.
- Follow Microsoft security blogs and announcements for new features and best practices in Microsoft 365 Defender, Defender for Cloud, and Sentinel.
- Participate in relevant online communities and forums to stay informed about real-world scenarios and emerging threats.

Troubleshooting Study Challenges

If you encounter difficulties understanding specific topics or concepts, consider the following approaches:

- **Re-read Sections:** Sometimes, a second reading can clarify complex information.
- **Consult Official Documentation:** The book provides a structured overview, but Microsoft's official documentation on Microsoft Learn offers deeper technical details and practical guides.
- **Hands-on Practice:** If possible, set up a lab environment (e.g., Azure trial subscription) to practice the configurations and scenarios discussed. Practical experience significantly aids comprehension.
- **Seek Community Support:** Online forums and study groups dedicated to Microsoft certifications can provide valuable insights and answers to specific questions.

Product Specifications

Title	Exam Ref SC-200 Microsoft Security Operations Analyst
Publisher	Microsoft Press
Publication Date	September 8, 2021
Edition	1st
Language	English
Print Length	336 pages
ISBN-10	0137568355
ISBN-13	978-0137568352
Item Weight	2.31 pounds
Dimensions	7.38 x 0.76 x 9.13 inches

Warranty Information

As an educational publication, this Exam Ref book does not come with a traditional product warranty. Its purpose is to provide comprehensive study material for the Microsoft SC-200 exam. The accuracy of the content reflects the state of Microsoft technologies at the time of publication. Users are encouraged to verify information against the latest official Microsoft documentation due to the dynamic nature of cloud services and cybersecurity.

Support and Additional Resources

For further support, official updates, and additional learning resources related to the SC-200 exam and Microsoft security technologies, please refer to the following:

- Microsoft Learn Official Website: The primary resource for Microsoft certification details, learning paths, and

documentation.

- **Authors' Resources:** While not directly linked in this manual, authors Yuri Diogenes, Jake Mowrer, and Sarah Young may provide additional insights or updates via their professional platforms or social media.
- **Community Forums:** Engage with the Microsoft Tech Community or other IT security forums for peer support and discussions.