Second Edition

CompTIA® CySA+ STUDY GUIDE

EXAM CS0-002

Includes one year of FREE access after activation to the online test bank and study tools:

2 custom practice exams
100 electronic flashcards
Searchable key term glossary

MIKE CHAPPLE
DAVID SEIDL

SYBEX
A Wiley Brand

Table of Contents

List of Tables

List of Illustrations

CompTIA®
Cybersecurity Analyst (CySA+) Study Guide
Exam CS0-002

Second Edition

Mike Chapple

David Seidl


SYBEX
A Wiley Brand

Published simultaneously in Canada and the United Kingdom

ISBN: 978-1-119-68405-3
ISBN: 978-1-119-68408-4 (ebk.)
ISBN: 978-1-119-68411-4 (ebk.)

Library of Congress Control Number: 2020937966

I dedicate this book to my father, who was a role model of the value of hard work, commitment to family, and the importance of doing the right thing. Rest in peace, Dad.

—Mike Chapple

This book is dedicated to Ric Williams, my friend, mentor, and partner in crime through my first forays into the commercial IT world. Thanks for making my job as a "network janitor" one of the best experiences of my life.

—David Seidl

Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank senior acquisitions editor Kenyon Brown. We have worked with Ken on multiple projects and consistently enjoy our work with him.

We also greatly appreciated the editing and production team for the book, including Kezia Endsley, our project editor, who brought years of experience and great talent to the project, Chris Crayton, our technical editor, who provided insightful advice and gave wonderful feedback throughout the book, Saravanan Dakshinamurthy, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book, and Liz Welch, our copy editor, who helped the text flow well. Thanks also to Runzhi “Tom” Song, Mike’s research assistant at Notre Dame who helped fact-check our work. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families and significant others who support us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Mike Chapple, Ph.D., CySA+, is author of the best-selling *CISSP* (*ISC*)^2 *Certified Information Systems Security Professional Official Study Guide* (Sybex, 2018) and the *CISSP (ISC)*^{2} *Official Practice Tests* (Sybex, 2018). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike is technical editor for *Information Security Magazine* and has written more than 25 books. He earned both his B.S. and Ph.D. degrees from Notre Dame in computer science and engineering. Mike also holds an M.S. in computer science from the University of Idaho and an MBA from Auburn University. Mike holds certifications in Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP).

David Seidl is Vice President for Information Technology and CIO at Miami University. During his IT career, he has

served in a variety of technical and information security roles, including serving as the Senior Director for Campus Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business, and he has written books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)*^{2} *Official Practice Tests* (Sybex, 2018) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests: Exam CS0-001*.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as certifications in CISSP, CySA+, Pentest+, GPEN, and GCIH.