Jump-start Your SOC Analyst Career

A Roadmap to Cybersecurity Success

Tyler Wall
Jarrett Rodrick

Apress®

Jump-start Your SOC Analyst Career

A Roadmap to Cybersecurity Success

Tyler Wall
Jarrett Rodrick

Apress®

Jump-start Your SOC Analyst Career: A Roadmap to Cybersecurity Success

Tyler Wall
Braselton, GA, USA

Jarrett Rodrick
Melissa, TX, USA

ISBN-13 (pbk): 978-1-4842-6903-9
ISBN-13 (electronic): 978-1-4842-6904-6
https://doi.org/10.1007/978-1-4842-6904-6

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-6903-9. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

This book is dedicated to our wives, Heidi and Stacey.

Table of Contents

About the Authors.....ix

About the Contributors.....xi

About the Technical Reviewer.....xiii

Acknowledgments.....xv

Introduction.....xvii

Puzzle Challenge.....xix

Chapter 1: The Demand for Cybersecurity and SOC Analysts.....1

Cybersecurity During a Crisis.....1

Demand for Cybersecurity Analysts.....3

Demand for SOC Analysts.....5

What This Book Is About.....7

Summary.....10

Chapter 2: Areas of Expertise in Cybersecurity.....11

Information Security.....11

Internal Teams.....15

External Teams.....20

Summary.....25

Chapter 3: Job Hunting.....27

Networking.....27

Applying for Jobs.....30

Common Interview Questions 32
Summary 36
Chapter 4: Prerequisite Skills 37
Networking 37
Network Security 43
Cryptography 44
Endpoint Security 45
Windows 45
MacOS 48
Unix/Linux 49
Other Endpoints 51
Summary 52
Chapter 5: The SOC Analyst 55
Tools 56
SIEM 57
Firewalls 58
IDS/IPS 58
Sandboxing 60
Definitions 62
Security Logs: Most Common 62
Security Event: Common 63
Incident: Uncommon 63
Security Breaches: Rare 63
Summary 64
Chapter 6: SOC in the Clouds 65
What Is Cloud Computing? 65
Types of Cloud Computing Deployment Models 67

Cloud Service Models 68

Evolution: Virtualization to Early Days of Cloud 70

Era of Virtualization 71

Early Cloud Development 71

Open Source Hypervisors and Cloud Development 72

Cloud Security 73

Conclusion 76

Chapter 7: SOC Automation 77

What Is SOC Automation? 77

Why Automate? 78

SOC Maturity 81

How to Start Automating 83

Sample Use Cases 85

Summary 87

Chapter 8: Real SOC Analyst Stories 89

Kaylil Davis, SOC Analyst 89

Toryana Jones, SOC Analyst 93

Brandon Glandt, SOC Analyst 95

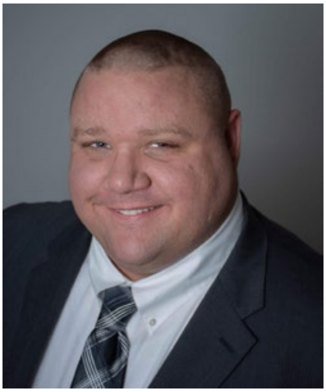
Matthew Arias, SOC Analyst 101

Rebecca Blair, SOC Director 105

Summary 108

Index 111

About the Authors



Tyler Wall is an accomplished security professional with years of experience in security operations and engineering that includes presently serving remotely as a Senior Security Engineer in Silicon Valley. He has led Security Operations Centers for global enterprises. His current focus is enabling Security Operations Centers to continuously mature by the adoption of security automation. Tyler's education includes a Master of Science in Cybersecurity Management, CISSP, CEH, CFSR, LRPA, Security+, Network+, and A+. He enjoys long golf cart rides in Braselton, GA, with his wife and son.

Jarrett Rodrick is the SOC Team Lead and Senior Information Security Analyst for VMware, the global leader in visualization technology. He's a retired Cyber Network Defender and Cyber Warfare Specialist from the US Army and has over 8 years of Defensive Cyber Operations experience working with the Army's Cyber Protection Brigade. Jarrett's time with the Cyber Protection Brigade has provided him with the skills needed to fight in today's cyberwar. Jarrett's cybersecurity certifications include GSEC, GCED, GCIH, GCIA, GCFE, GCFA, GSNA, GRID, GCUX, and GSTRT. Jarrett lives in Melissa, TX, with his wife and family and enjoys researching new and innovative technologies.

About the Contributors

Anand Purohit has been working in IT for over 15 years with the past 8 years focused on Technology and Cloud Strategy, Architecture, and Governance. He has held various executive roles within consulting, healthcare, and financial services working closely with peers in cybersecurity, risk, and compliance while transforming organizations' technology operating model using cloud (public, private, or hybrid). Anand graduated from Stevens Institute of Technology and now lives in Atlanta with his wife and son.

Jason Tunis is a Lead Security Operations Center analyst at Aegon with over 12 years of cybersecurity experience. He spends his time primarily focused on incident response, cyber threat intelligence, and security automation. Over the past 2 years, Jason has helped to build a highly skilled Security Operations Center. Jason lives in the Midwest with his wife and three children.

About the Technical Reviewer

Mark Furman received his MBA from Ohio University and a Bachelor of Science in Information Technology from Purdue University. He has worked in the IT and cybersecurity field for over 19 years. Some of his accomplishments include writing and publishing a book on virtualization, participating as a technical editor for books, starting a successful cybersecurity program at a technical college, and launching a business incubator and makerspace. Currently, Mark is in the process of launching a new cybersecurity company called Kaldara Security.

Acknowledgments

First, I would like to acknowledge Apress for understanding the vision of this book: to make the impossible possible.

I would also like to acknowledge my employer VMware for the time and creative space to express my ideas. Additionally, I would like to acknowledge my leadership chain for their input concerning this book. VMware is a terrific company, and I believe in EPIC2 values which include community, the very cornerstone of this book.

I would like to humbly thank and acknowledge the few influential people in my life. My wife, Heidi. I would also like to thank my father, Peter. My mother and stepfather, Karen and Kenny. Sister and brother, Ginny and Lew. My friends, Steven C., Stephen S., Spencer R., Frank F., Andy W., Fred S., Dwight F., Philip S., Sam C., Chris P., Reese and Mike W., Daniel W., and Corey Milford and the Milford Team. I would like to thank my mother-in-law, Lori, and her mother Mary. I would like to extend that gratitude to my sister-in-law and her husband Shuvo. I would like to show thanks to my cousins Justin, Alan, Trey, Dana, and Michael and their kids. I would like to acknowledge my uncle, Edd. Lastly and in conclusion, I would like to thank my uncle, Chuck, for his most honorable service to this country and our family.

—Tyler Wall

First and most important, I'd like to thank my beautiful and loving wife, Stacey. Your constant supply of love and patience has provided me with the needed support to become the Cyber professional I am today. Thank you!

I’d also like to thank the countless Soldiers and Army Leaders I’ve had the pleasure to learn from in my 16-year career. From my Drill Sergeants at Fort Knox to the Senior Officers at the Cyber Protection Brigade, you’ve all played a pivotal role in my development. Thank you!

Finally, I’d like to thank VMware, for taking a chance on a soon-to-retire Soldier and offering me a career outside of the Army. I truly couldn’t have asked for a better company to work for. Thank you!

—Jarrett Rodrick

Introduction

Welcome to the wonderful world of *Jump-start Your SOC Analyst Career*! You picked this book up because you want to get into the action! Into the money! Into the challenges that lie ahead! We will tell you how wonderful and rewarding this career is, but first let us say something about infosec. If you get into the cybersecurity industry and you aren't connected to the community, you are missing out. There are all kinds of micro infosec communities and communities for special groups of people, but in contrast there are communities that want to include everyone. There are extremely esoteric communities filled with mystery and secrets, there are communities for just CISOs and communities for just engineers, there is a military community, communities for Bill and Bob, communities for the government sector, a community of breakers and makers alike… if there is only one common trait that people coming into security want, it is a sense of community - and infosec has it! It is really hard to relate to people in the normal world sometimes, especially if you are starting out and keyboarding alone. We promise you there are many other people that want to keyboard alone next to you. It happens all the time at conferences! There are so many amazing people in the community, and sometimes they don't always get along, but in 3–6 months, it will be like it never happened. Our goal for this book is to get you in the chair in the SOC you dream about and open your eyes that no matter who you are, cybersecurity is for you.

This book will cover what you need to know that we have deemed to be important to know as a SOC analyst. There are a lot of open jobs in cybersecurity, but there are also a lot of candidates that want those jobs. The challenge is that there are not a lot of the right kind of candidates to fill them. We explain to you what the right kind of candidate is and give you