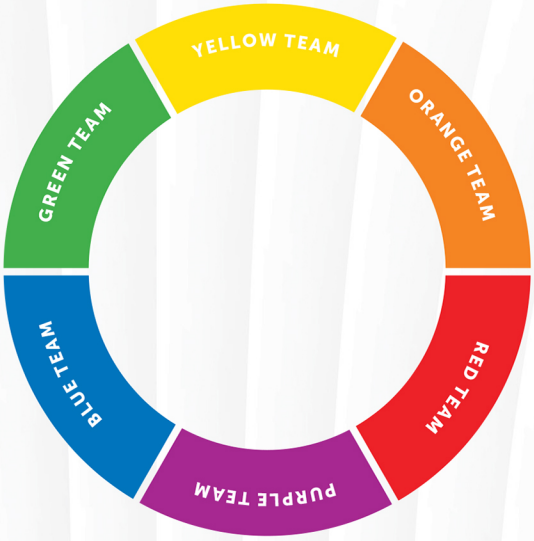

SEE YOURSELF IN CYBER

SECURITY CAREERS **BEYOND HACKING**

ED ADAMS

WILEY

SEE YOURSELF IN CYBER

SEE YOURSELF IN CYBER

Security Careers Beyond Hacking

ED ADAMS

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394225590 (Hardback), 9781394225613 (ePDF), 9781394225606 (ePub)

Library of Congress Control Number: 2023952256

Cover image: © bgblue/Getty Images
Cover design: Wiley

To my wife, Maureen, without whom none of this would be possible.

You are not only the light that shines our way to give us clear vision; you are also the rock-solid foundation upon which we stand and build, together, our life. All of my many projects and side projects—you abide, support, enable, and enhance.

Thank you for being so loving, critical, patient, and creative. You challenge me to be better in every way; I am so very blessed and fortunate to have you by my side.

Contents

Part I

The Many Colors of Cybersecurity

Part I of this book explains the many work roles that can, do, should, and might incorporate security as an aspect of the job. I use the analogy of the color wheel to create the *cybersecurity color wheel*, which is split into six segments: the primary colors of red, blue, and yellow, followed by the secondary colors of purple, orange, and green. I also include a chapter solely dedicated to the color white, which sits at the center of the cybersecurity color wheel, touching each of the six color slices.

For the primary colors, I relate many jobs to the Workforce Framework for Cybersecurity (the NICE Framework), as it is one of the few comprehensive efforts that document cybersecurity work roles and the associated knowledge, skills, activities, and tasks associated with each one. However, the NICE Framework is not an accurate depiction of today's cybersecurity workforce. I point out the relevant differences where most appropriate and provide real-world examples of jobs, responsibilities, and career paths in these color slices.

For the secondary colors, the NICE Framework has virtually no coverage when it comes to work roles; however, these colors provide exciting potential for cybersecurity professionals and those interested in integrating security activities into non-security-specific jobs.

The final chapter of Part I is all about the jobs that provide the vision and guardrails for the cybersecurity work done at a given organization. These are the professionals who collect, collate, analyze, and disseminate the security and privacy requirements placed upon the enterprise, translating them into controls for each major workgroup.

Chapter 1

Introduction and Motivation

I am an imposter.

Many people consider me an expert in cybersecurity, particularly software/application security. Yet, I have no degree in cybersecurity. I have zero security industry certifications. I have never been a cybersecurity practitioner for an enterprise or government agency. So I'm a phony, right? A fraud.

Wrong! Like many of us in this industry, I am mostly self-taught. I leveraged the education and experience I had to build the body of knowledge that has become my own—vast and broad and uniquely "Ed." Nobody has the experience and education that I do. I have proven myself time and time again. I am a trusted advisor to my clients, I am a speaker at industry conferences, I am a cybersecurity talk show host, and I am a sought-after expert for that very knowledge and experience only I have. I belong.

Many of us in cybersecurity feel conflicted. We feel as if we don't belong because we haven't "earned our stripes" or we lack some technical degree, certification, or hands-on experience. Imposter syndrome is real. But I'm writing this to let you know that you don't need a technical degree or any particular certification or prior hands-on experience before starting your career in cybersecurity. Cybersecurity has hundreds of different types of jobs, both technical and nontechnical. I have many friends and colleagues in cyber (many

holding C-level positions) who graduated with degrees in Spanish, finance, philosophy, and other nontechnical/engineering disciplines. I have undergraduate degrees in mechanical engineering and English literature, as well as a master's in business administration (MBA). Nothing in my education would lead one to think I'd become a cybersecurity "expert"—yet here I am writing this book after spending the past 20 years in the security field. And I love it. You can too.

As executives, hiring managers, HR professionals, and others who create cybersecurity job descriptions and hire practitioners, we need to be mindful that we reflect realistic requirements for job seekers. One of my good friends, who is a CISO, reminds me that she has seen far too many entry-level jobs that require Certified Information Systems Security Professional (CISSP) certification, for example. The CISSP certification requires five years of industry experience before you can even sit for the exam. These paradoxical blockades abound in the cybersecurity industry; it is our obligation and duty to correct them.

How This Book Is Organized

I've organized this book into two parts, covering the following main topics:

- **In Chapters 2–5, we explore cybersecurity careers using the analogy of the color wheel:** I first came across this concept when I saw April Wright deliver a brilliant talk at the 2017 BlackHat USA conference.[1] Other folks, like Louis Cremen in

[1] *Orange Is The New Purple*, by April C. Wright For BlackHat USA 2017, `www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf`.

2020,[2] expanded on Ms. Wright's talk, and I plan to do the same. I'll discuss cybersecurity via primary colors first (red, blue, and yellow) followed by the blended secondary colors (purple, orange, and green). I also spend time talking about the absence of color in cybersecurity: white jobs. For each of these, I reference what I consider to be the most comprehensive research published on cybersecurity jobs: *The Workforce Framework for Cybersecurity,* commonly referred to as the NICE Framework (see `https://niccs.cisa.gov/workforce-development/nice-framework`), published as part of the National Initiative for Cybersecurity Careers and Studies (NICSS) under the purview of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). But the NICE Framework is flawed. It doesn't include many common jobs that relate to cybersecurity, and it doesn't address how to incorporate security into noncybersecurity jobs, a crucial necessity for defending our digital enterprises.

- **In Chapter 6, we cover software:** We can't operate today without the enablement of software, so I dedicate a chapter to it and highlight its importance. Regardless of which job you want in cybersecurity, it will be difficult to avoid dealing with software at some level. Most simply it is the fuel for our connected digital world. The vast majority of cybersecurity jobs do not require knowledge of how to code; however, a basic understanding of how software works, as well as how and where it enables technologies such as the Internet of Things (IoT),

[2] *Introducing the InfoSec Colour Wheel—Blending Developers with Red and Blue Security Teams*, by Louis Cremen, `https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-evelopers-with-red-and-blue-security-teams-6437c1a07700`.

blockchain, and the cloud is essential. Say you take a job as a cyber audit or risk professional. Without the ability to assess how the software in scope complies with the standards against which you're measuring, you won't be able to do your job effectively.

- **In Chapter 7, we cover diversity and inclusion:** This is a passion of mine. My demographic, middle-aged white males, dominates the cybersecurity workforce in terms of percentage employed. This is a dangerous cybersecurity problem as much as it is a socioeconomic issue. More diverse teams make better decisions, operate more efficiently/profitably, and outperform homogeneous groups; this has been proven in numerous studies. Meanwhile, the cybersecurity industry has millions of unfilled job openings. We have an opportunity to address multiple challenges at once. This is discussed at length in Chapter 7.
- **In Chapter 8, I include interviews and survey results from working cybersecurity practitioners:** One lesson I've learned in my career, sometimes painfully, is that I often need help. Some of the smartest, most successful people I know are quick to point to others who have enabled them, supported them, and otherwise assisted them. I interviewed dozens of cybersecurity professionals and asked them the same set of questions about their origin, what they look for when hiring, and challenges they've faced. I share those insights in this chapter along with data collected from online surveys asking the same questions.

Who This Book Is For

This book has a twofold objective, discussed in the following sections.

For Managers, Directors, Executives, and Other Business Leaders

You'll learn to create a relatable framework for the dozens of cybersecurity jobs that exist. Complement the work done by others, for example, the National Initiative for Cybersecurity Education, with practical experience to help build an understanding of realistic expectations, job descriptions, and recruiting strategies. I also provide insights and views into the many different ways the people in your organization—inhabiting a variety of roles not traditionally associated with cybersecurity—can contribute to improving its cybersecurity backbone. You'll discover how developers, DevOps professionals, managers, and others can strengthen your cybersecurity. You'll also find out how improving your firm's diversity and inclusion can have dramatically positive effects on your team's talent. The book should also be valuable to policymakers, regulators, and compliance professionals who want to better understand the roles, responsibilities, tasks, and contributions various job functions provide to cybersecurity hygiene.

For Individuals Interested in Entering the Industry or Furthering Their Cybersecurity Career

You'll learn to create a similarly relatable framework for cybersecurity jobs, particularly those you might not be aware of. Cybersecurity is popularized by the hackers and defenders. Imagery of black hoodies or massive war rooms with ceiling-high screens showing threat intelligence are commonplace when people imagine cyber. But the reality of the industry can be far more mundane—and far more interesting to those not drawn to hacking and war rooms. If you have a background in finance, legal, psychology, law enforcement, or economics (just as a few examples), you can build a lucrative career in cybersecurity. I also want to paint several pictures for you about the

world of cybersecurity that might help broaden your perspective and pique your interest further than where it is now.

About the NICE Framework

The National Institute of Standards and Technology (NIST) developed *The Workforce Framework for Cybersecurity,* also known as the NICE Framework (see `https://niccs.cisa.gov/workforce-development/nice-framework`). It attempts to be a comprehensive guide to identify and categorize various work roles within the realm of cybersecurity. Its structured approach can help organizations define cybersecurity-related tasks, skills, and competencies required for a successful workforce. It doesn't perfectly reflect job titles that exist in the industry, but I attempt to augment them with actual work roles in each of the color slices covered in this book.

The NICE Framework has three major components:

- Seven categories that provide a high-level grouping of common cybersecurity functions
- Thirty-three specialty areas meant to define distinct areas of cybersecurity work
- Fifty-two work roles, a detailed grouping of cybersecurity jobs comprised of specific *knowledge*, *skills*, and *abilities* (KSAs) required to perform the work

The work roles and related KSAs are valuable resources for any cybersecurity or human resources leader when contemplating job descriptions, performance evaluation, and career pathing. It is also incredibly useful for job seekers looking to enter or further their career in cybersecurity.

The following are the seven categories of the NICE Framework:

- Securely Provision
- Operate and Maintain
- Oversee and Govern
- Protect and Defend
- Analyze
- Collect and Operate
- Investigate

Some of those phrases don't really jibe with day-to-day job functions. To help, let me translate a couple into more recognizable terms:

- **Securely Provision:** This means build or buy. Think developers (both software and IT system), architects, testers/quality assurance, product managers, procurement teams, and to some extent risk managers (although I could put them in a few of the categories). In the world of DevOps, this is "Dev."
- **Operate and Maintain:** This is your IT system and network operations team. Think system administrators, tech support, and DBAs. In the world of DevOps, this is "Ops."
- **Oversee and Govern:** This is the team that provides leadership and guidance for cybersecurity across all teams. Think C-suite, legal, policy and planning, and, very importantly, security training and awareness.
- **Protect and Defend:** This is the core of day-to-day cybersecurity for many practitioners. It's all about cyber defense, incident response, vulnerability assessment, and management of the

security holes identified in the supported IT systems. Here you'll find security operations center (SOC) analysts, penetration testers, security engineers, and many jobs on the information security team.

- **Analyze:** This is a weird one for me because virtually every cybersecurity job function has an analyze component. NICE includes activities such as threat intelligence, exploitation analysis, threat modeling, and even cultural analysis applied to cybersecurity. The work roles NICE lists under this category seldom exist in practice. The most common I see is the threat intelligence analyst (or something of that ilk).
- **Collect and Operate:** This is another oddball. NICE describes this as "specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence." I witness this applied in nearly every job function that incorporates security considerations. Devs restrict user input, Ops use firewalls to block certain traffic, Govern defines what can/can't be collected, and so forth. Similar to the Analyze category, I seldom see the work roles NICE list in practice; for example, All Source-Collection Manager (CO-CLO-001) is a job I've never seen listed. Maybe once or twice the term has come across my radar screen as part of a U.S. Department of Defense job posting, but I'm confident it's only in that specific niche and only because of the NICE Framework. Otherwise, the job title simply doesn't exist as part of the cybersecurity industry.
- **Investigate:** This is all about surveillance and forensics. Think cybercrime investigator, digital forensics analyst, special agent (for FBI), and so on. This category is closely related to the world of incident response.

For each of the chapters in which I discuss careers related to a color, I reference the NICE-defined work roles as well as roles I know to exist in practice. Knowing both will help you align your objectives with both an academic/research-based publication as well as the experience of someone with 20 years in the industry who has recruited, hired, and developed hundreds of professionals, either directly or indirectly, related to cybersecurity.

Summary

Now that you've read my motivation for writing this book and understand how it is organized, I hope you will dive in with enthusiasm, ready to learn more about the exciting field of cybersecurity. I have enjoyed the field for the better part of two decades; yet, many remain vexed and confused by cybersecurity jobs and career paths. I have seen far too many cybersecurity leaders, hiring managers, and HR professionals write job descriptions that are fantastical. The result is the disenfranchisement of potential hires who could actually perform very well in the job had it been appropriately described.

We all need to be more mindful to create more realistic requirements for our cyber needs. Cybersecurity leaders can use this book as a reference guide to glean valuable insight into work roles and the associated knowledge, skills, abilities, and tasks for each one related to security. Also, read Chapter 7 on diversity and inclusion with an open mind, as it may provide you with useful tools to cultivate, attract, develop, and retain a more diverse and happy staff. Finally, read how practitioners responded to the interview questions I posed and consume the case studies with an eye toward replicating such success and inspiration in your own organization.

Many individuals keen to learn more about cybersecurity careers don't know where to turn. This book endeavors to provide a plethora

of useful information, references, and stories meant to educate, inspire, assist, and hire practitioners. If you are one of these individuals, you can flip through Chapters 2–5, which discuss the cybersecurity color wheel, to learn about jobs related to each color slice. Also, feel free to jump straight to the special subject chapters dedicated to software, diversity, and inclusion, or the advice and case studies.

Chapter 2

The Many Colors of Cybersecurity

In the dynamic realm of cybersecurity, roles and responsibilities span a vast spectrum, encompassing everything from analyzing threats to governing policies and innovating solutions. To better understand this intricate landscape, I draw inspiration from the color wheel, as others before me have. This visual representation of primary and secondary colors blend to create a comprehensive palette of cybersecurity jobs and noncybersecurity jobs alike. For noncybersecurity jobs, I discuss the security aspects of those jobs and how very important they are to executing quality work for that particular function.

As discussed in the previous chapter, *The Workforce Framework for Cybersecurity*, also known as the NICE Framework, serves as a comprehensive guide for identifying and categorizing various work roles within the realm of cybersecurity. Its structured approach aids organizations in defining cybersecurity-related tasks, skills, and competencies required for a successful workforce.

The NICE Framework and the Color Wheel

Just as colors combine to form a harmonious spectrum, the NICE Framework brings together diverse work roles to fortify the digital realm. In this chapter, I explain each of the primary and secondary

colors and relate them to four major groups: builders, breakers, defenders, and bakers.

In the following chapters, I embark on a journey to relate NICE Framework work roles to the primary and secondary colors of the color wheel, unveiling a creative perspective on the intricacies of cybersecurity roles and their interconnectedness. I then augment the NICE work roles with sample jobs that exist in the industry but are omitted by the NICE Framework by name (either accidentally or because they are assumed to be subsumed as part of one of the NICE work roles).

April Wright's presentation at the BlackHat USA 2017 conference introduced the concept of the Information Security Color Wheel, a visual framework that helps organizations determine the appropriate levels of security measures based on the sensitivity of their data and systems. The color wheel analogy offers a simplified and effective way to communicate security requirements and priorities to stakeholders within an organization. Louis Cremen, a software developer turned security professional, added to Ms. Wright's color wheel concept by including and blending developers into the infosec circle. The world of information security is dominated by two main groups: red and blue. See Figure 2.1.

The red team is made up of employees or contractors hired to be *breakers*. These ethical hackers work to find security vulnerabilities that a malicious actor could exploit. Their complement, the blue team, are *defenders*. They are responsible for protecting an organization with cybersecurity defenses, such as firewalls and other intrusion prevention systems. As you'll learn later, combining red and blue teams creates a purple team effect, which can exist independently or as part of either a red or blue team, but more on that later.

When Mr. Cremen added the yellow team to the color wheel, he primarily referred to software engineers. Undoubtedly, software engineers are the largest and arguably most influential group in this

color slice; however, I prefer to include other types of developers too—for example, IT systems architects, network designers, engineers, and so on. I refer to this group as *builders*. These are people who design and construct software, systems, and integrations that make enterprises more efficient. Their focus is often on implementing requirements (features), and a major pressure point for this group is delivery timelines. With respect to quality, the focus tends to be on functionality, usability, reliability, and performance. Security is a natural add-on to their quality considerations. Further combining red or blue into these yellow teams creates the emerging secondary cyber colors of green and orange. I discuss each of those separately in the coming chapters.

Figure 2.1 Ed Adams cyber color wheel

For all the building, breaking, and defending going on in any given enterprise, there needs to be some form of guiderails. These recipes are provided by a group I refer to as *bakers*. These are the people who collect, collate, and disseminate the security and privacy requirements placed upon the enterprise. These requirements can