



BUILDING A CAREER IN CYBERSECURITY

THE STRATEGY AND SKILLS YOU
NEED TO SUCCEED



YURI DIOGENES

Foreword by **MERAV BAHAT**, CEO and Co-Founder of Dazz

FREE SAMPLE CHAPTER |



BUILDING A CAREER IN CYBERSECURITY

This page intentionally left blank

BUILDING A CAREER IN CYBERSECURITY

The Strategy and Skills
You Need to Succeed

YURI DIOGENES

◆ Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi
Mexico City • São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2023939921

Copyright © 2024 Pearson Education, Inc.

Cover image: M-vector/Shutterstock

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

ISBN-13: 978-0-13-821451-7

ISBN-10: 0-13-821451-4

ScoutAutomatedPrintCode

Editor-in-Chief

Mark Taub

Executive Editor

Loretta Yates

Associate Editor

Shourav Bose

Development Editor

Rick Kughen

Project Editor

Mary Roth

Copy Editor

Rick Kughen

Indexer

Timothy Wright

Proofreader

Barbara Mack

Technical Reviewer

Nicholas DiCola

Cover Designer

Chuti Prasertsith

Figure Credits

Figures 1.3, 1.4: Cyberseek US

Figure 1.5: Glassdoor, Inc

Figure 2.1: Bleeping Computer LLC

Figure 2.4: Keith Bell/Shutterstock

Figures 3.4-3.7: Wireshark Foundation

Figure 4.4: X Corp.

Figure 5.1: Net Vector/Shutterstock

Figure 5.2: zieusin/Shutterstock

Figure 5.3: tkemot/Shutterstock

Figure 6.4: iQoncept/Shutterstock

Figure 7.1: rostislavsedlacek/123RF

Figure 7.2: Panchenko Vladimir/Shutterstock

Figure 7.3b: Illustration Forest/Shutterstock

Figure 8.1: elnur/123RF

Figure 8.3: kasahasa/Shutterstock

Figures 9.2-9.4: Indeed

This page intentionally left blank

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

Dedication

I dedicate this book to all my students that are always asking me questions with the intent to learn more about cybersecurity and be a better professional.

CONTENTS AT A GLANCE

Foreword	xiv
Introduction	xv
Acknowledgments	xvii
About the Author	xvii
I Starting Your Career in Cybersecurity	1
1 The Cybersecurity Universe	3
2 Establishing a Plan	25
3 Building Your Lab	45
4 Networking	65
5 Interview	83
II On the Job	97
6 Your Employer Is Your Customer	99
7 Dealing with Obstacles	111
8 Growing in Your Career as a Remote Worker	127
9 What's Next in Your Career?	139
10 Owning a Cybersecurity Business	149
Index	161

TABLE OF CONTENTS

Foreword	xiv
Introduction	xv
Acknowledgments	xvii
About the Author	xvii
I STARTING YOUR CAREER IN CYBERSECURITY	1
1 The Cybersecurity Universe	3
Cybersecurity Careers	4
Cybersecurity Roles and Responsibilities	5
Cybersecurity Jobs	8
Cybersecurity Skills	12
Navigating the Industry	17
Summary	23
2 Establishing a Plan	25
Explore Your Current Skills	26
Create Your Plan	30
Organizing Your Plan	32
Cybersecurity Certifications	34
Foundational Security Certifications	36
Cybersecurity Analyst and Security Practitioners Certifications	40
Specializations	42
Vendor-Specific Certifications	43
Summary	44
3 Building Your Lab	45
Lab Requirements	46
Creating Your Lab	49
Scenario 1—Operating Systems Process	49
Scenario 2—Network Traffic Analysis	52
Scenario 3—Cloud Security Posture Management	56
Scenario 4—Multi-Cloud Security	57
Scenario 5—Regulatory Compliance	57

Scenario 6—Attack Simulation	57
Scenario 7—Security Information and Event Management	58
Scenario 8—Threat Hunting	59
Scenario 9—Threat Intelligence	59
Self-Assessment	60
Summary	63
4 Networking	65
Networking in Cybersecurity	66
Look Inward	69
Online Presence	73
LinkedIn	74
YouTube	75
Twitter	76
Searching for a Job	77
Summary	82
5 Interview	83
Technical and soft skills	84
Interview process	84
Initial triage	85
Prepare for the interview	85
Formal interview rounds	88
Interview questions	90
Final decision	93
Summary	95
II ON THE JOB	97
6 Your Employer Is Your Customer	99
Cybersecurity Goes Beyond Technology	100
Organizational Structure	102
Responsibilities and Expectations	103
Mapping Your Responsibilities	104
Plan to Conquer	105

	Entrepreneur Mindset.....	106
	Summary.....	109
7	Dealing with Obstacles	111
	Obstacles in Cybersecurity.....	112
	Unconscious Bias and Cybersecurity.....	115
	Adjusting Your Cybersecurity Skills.....	117
	What Got You Here Won't Get You There.....	119
	Work-Life Balance in Cybersecurity.....	119
	Growing at a Healthy Pace.....	122
	Time Management.....	124
	Summary.....	126
8	Growing in Your Career as a Remote Worker	127
	The Growth of Remote Workers.....	128
	Hybrid Work.....	130
	Making an Impact as a Remote Worker.....	131
	Influencing Others.....	132
	Actively Look for Feedback.....	133
	Staying Active.....	134
	Transparency.....	136
	Summary.....	137
9	What's Next in Your Career?	139
	Moving Up or Moving Laterally?.....	140
	Self-Assessment.....	142
	Evaluating the Options.....	143
	Upcoming Cybersecurity Opportunities.....	144
	Keep Moving Forward.....	148
	Summary.....	148

10	Owning a Cybersecurity Business	149
	Knowing More about the Guest Authors	150
	Stepping Stones to Flying Solo	152
	Paula Januszkiewicz’s Keys to Entrepreneurial Success	153
	Key Elements for Success	154
	Common Pitfalls and Challenges	156
	David Kennedy: Starting from the Ground Up	158
	Final Considerations	160
	Summary	160
	Index	161

Foreword

We live in a world where cybersecurity events are daily, front-page news — zero-day vulnerabilities in software supply chains, stolen credentials, attacks on hospitals, gas pipeline shut-downs, and school ransomware events. As we've become a more digital and connected global economy, the number of attacks has increased with no sign of slowing down. The need for people working in cybersecurity has never been more acute.

While my background as a cybersecurity leader is more traditional, coming from both military and engineering, I actually began my career in information technology. However, early on, I realized the huge potential of the cybersecurity industry, fell in love with the mission, and developed a great passion for the domain. There is no one path to the field. In fact, there are many ways to get started, whether your background is in engineering, education, law, criminal justice, marketing, sales, finance, or human resources.

You could be part of a technology startup like Dazz, which builds innovative products and services to help organizations discover, reduce, and fix security risks. For women, in particular, who have low representation in cyber, I encourage you to join startups in their early stages, when most of the learning takes place.

Alternatively, you could be a practitioner and get hands-on with technology or intelligence as a cybercrime investigator, ethical hacker, red team tester, researcher, security architect, or information security leader inside a company, school, hospital, or government.

Whichever path you take, you'll stretch and grow, learn new things, and gain fulfillment knowing you are working for the greater good of society.

You are in good hands with my friend and colleague, Yuri Diogenes, on how to begin your journey. There is high demand for skilled cybersecurity professionals, which is only expected to grow in the coming years. I encourage you to join us and experience one of the most rewarding careers you could embark upon.

*Merav Bahat
Co-founder and CEO
Dazz*

Introduction

Coming from a background in information technology, and more specifically, computer networks, the migration to cybersecurity was very smooth because I had a good foundation in two critical areas: operating systems and networking. However, I didn't understand the options available in this field or what gaps I needed to fulfill before applying for a cybersecurity-related position. I had no idea where to start. To this day, I believe I spent too much time focusing on the wrong things, and my cybersecurity career took a little longer to take off. In addition to my personal experience entering this field back in 2006, I keep seeing a trend among my university students who frequently ask for guidance on either improving in this field (if they are already in cybersecurity) or how to migrate from a different area to cybersecurity. These trends not only match my own experience but also match common questions brought to me by my mentees at work.

Based on these experiences, I decided to start this project, and when I was writing the table of contents for the book, I also reflected on the areas I took for granted but were critical in my career growth, such as soft skills. I decided to frame the book so that it is not only about cybersecurity per se but how to be a complete cybersecurity professional who can add value to the business, both from a technology and overall package perspective. As a manager in my company, I see many candidates hired because they were complete candidates — soft skills, attitude, mindset, and technical abilities — not because they had the best technology resumes.

My experience as a cybersecurity professional, university professor, and manager has allowed me to share different dimensions of what it takes to build a solid career in cybersecurity. However, I wanted to ensure that I had the right team to be part of this project, so I invited Nicholas DiCola, VP of Zero Networks and my former manager at Microsoft, to be the technical reviewer for the book. Nicholas has a lot of experience in this field, and throughout this project, he gave me extra tips to include in the book. I also invited Merav Bahat, co-founder and CEO of Dazz, a cloud security startup, to assist. I worked with Merav at Microsoft, where she was directly responsible for my career growth to the next level. I also wanted to incorporate some entrepreneurship vision to show that you can start your own cybersecurity business, so I invited Paula Januszkiewicz and David Kennedy to lend their perspectives. Paula and David are two great cybersecurity professionals with their own cybersecurity businesses.

I hope that the hours we invested in this book are valuable to you and you can finish this book with a good plan of action to pursue your cybersecurity career and become a better professional.

Good luck!

Yuri Diogenes

Register your copy of *Building a Career in Cybersecurity* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to informit.com/register and log in or create an account. Enter the product ISBN (9780138214517) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

Acknowledgments

I would like to thank my wife and daughters for their endless support; my great God for giving me strength and guiding my path on each step of the way. Thanks to my mother, for always emphasizing to me the importance of education and study. To my coworkers and former managers that contributed to my career progress, especially Cyndee Young, Rebecca Halla, and Sonia Wadhwa.

I want to thank my friend Nicholas DiCola for the great work reviewing this book, friendship, and guidance over the years. Thanks to Merav Bahat for writing the foreword of this book and for her inspiring career and leadership. Thanks to my friends Paula Januszkiewicz and David Kennedy for your amazing contributions to Chapter 10. Thanks for bringing your vision and valuable insights. I truly appreciate it.

Thanks to Pearson's team, especially Loretta Yates and Rick Kughen, for another amazing partnership.

About the Author

Yuri Diogenes has a master of science in cybersecurity intelligence and forensics investigation from UTICA College and is working on his Ph.D. in cybersecurity leadership from Capitol Technology University. Yuri has been working at Microsoft since 2006 and is a principal PM manager for the Customer Experience Engineering Defender for Cloud team, where he manages a global team of product managers focusing on cloud security posture management and workload protection. Yuri has published more than 30 books, mostly about information security and Microsoft technologies. Yuri is also a professor at EC-Council University, where he teaches in the cybersecurity bachelor's program. Yuri also has an MBA and many IT/Security industry certifications, such as CISSP, MITRE ATT&CK Cyber Threat Intelligence Certified, E|CND, E|CEH, E|CSA, E|CHFI, CompTIA Security+, CySA+, Network+, CASP, and CyberSec First Responder. You can follow Yuri on Twitter at @yuridiogenes.

This page intentionally left blank

Building Your Lab

“Knowledge is of no value unless you put it into practice.”

–Anton Chekhov

Now you know what you want. You have identified the cybersecurity area you want to work in, identified your current gaps, and established a plan. As part of this plan, you should have added time to ramp up with the technology areas in which you need to improve.

However, you can read about these technologies all day long, but if you don't do hands-on practice, your knowledge will be limited, which might affect you while interviewing. When you don't have hands-on experience in a subject, it's hard to feel confident that you can actually implement the things you just learned about in theory.

With the number of online resources we have nowadays, it's easier to create your own lab to implement scenarios that will help you gain more experience. This chapter will assist you in creating a lab and suggest some scenarios you can use to put things into practice.

Lab Requirements

While different cybersecurity jobs will require different skills, the goal here is to ensure that you have a good foundational understanding of technologies that can be utilized across different cybersecurity job roles. Building this foundational lab allows you to continue adding new scenarios to learn different skills.

To create this foundational lab, you need to cover some core scenarios, and based on these scenarios, you will have the minimum requirements for this lab. Table 3.1 highlights what's covered in each of the scenarios in the lab I'm proposing:

Table 3.1 Lab scenarios and requirements

Scenario	Level	Minimum requirements
Understand operating system processes and threads	Basic (100)	One virtual machine (VM) Windows operating system (OS) Process Monitor by Sysinternals
Understanding the communication between two hosts in the same TCP/IP subnet	Basic (100)	Two virtual machines (VMs) Windows OS Wireshark
Cloud security posture management	Intermediate (200)	Azure subscription Microsoft Defender for Cloud

Scenario	Level	Minimum requirements
Multicloud security posture management	Intermediate (200)	Azure subscription AWS account GCP project Microsoft Defender for Cloud
Understanding regulatory and compliance standards	Intermediate (200)	Azure subscription Microsoft Defender for Cloud
Simulating and detecting attacks on Windows and Linux	Advanced (300)	Azure subscription Linux OS Microsoft Defender for Servers Four virtual machines (VMs) Windows OS
Implementing a cloud-based security information and event management (SIEM)	Advanced (300)	Azure subscription Microsoft Sentinel
Threat hunting	Advanced (300)	Azure subscription Microsoft Defender for Cloud Microsoft Sentinel
Gathering threat intelligence	Advanced (300)	Azure subscription Microsoft Sentinel MITRE ATT&CK Framework



Note

While you can use other tools for these scenarios, most enterprise-level security tools require a license, and trial versions of the Microsoft products shown in Table 3.1 are available. These allow you to learn without having to pay for the software. One alternative for an open-source lab is <https://labs.fedoraproject.org/en/security/>.

One important thing to mention about Table 3.1 is that the suggested minimum requirements are based on the material I cover in this chapter. However, nothing stops you from adding other elements to this scenario. For example, in implementing a cloud-based security information and event management (SIEM) scenario, the minimum requirement is to use a Microsoft SIEM solution called Microsoft Sentinel. However, you can build your own lab to use another solution, such as Splunk.

While thinking about potential additions to each scenario, consider whether those additions will cost money. My intent is to help you build a free lab to practice. Remember that once you start deploying these solutions, your clock starts, and you need to finish everything in a specific time frame since some of these solutions are free only during a trial period. That's why it is so important to clearly define everything you want to test and practice during this ramp-up phase. Figure 3.1 has an example of how you can plan your trial usage, assuming a 30-day trial (which is the case for most of the products used in this lab):

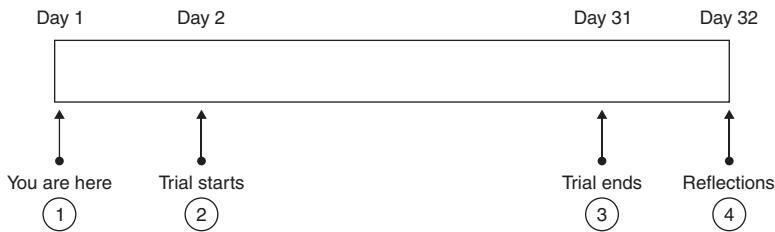


Figure 3.1 *Roadmap to conclude the lab*

The diagram shown in Figure 3.1 has four major phases:

- **You are here:** This is where you are right now, reading this chapter and defining which scenarios you want to implement. For example, if you are already an IT professional migrating to cybersecurity, you might not need to implement scenarios 1 and 2.
- **Trial starts:** Once you have enumerated which scenarios you want to implement, then you can start deploying the products, which usually entails starting the trial period for that product and also for the platform (in this case, Azure).
- **Trial ends:** Add the ending date on your calendar, and add a calendar reminder at least 10 days before the trial expires. Some of these products will require you to supply a credit card number when you sign up for a trial. While they don't charge you upfront if you go over the 30 days, they will start charging for the next cycle. So, make sure

to cancel your subscription before the 30th day of use. This 10-day reminder prompts you to evaluate what you have done so far and whether anything is missing. If you've already implemented all scenarios and are ready to move on, just cancel the subscription.

- **Reflections:** After everything is done, you should pause for a day and reflect on the lessons learned. A good way to practice what you've learned is to write a report with your observations about each scenario. This report should contain more than just copy-and-pasted material from articles you read to help you with the lab. Instead, it should include your thoughts about what you have learned and whether you believe there are still some areas you need to continue improving as you move forward. This report will also help you to prioritize the areas you need to improve and the areas where you already feel confident.

The following sections will go over each scenario. Some scenarios will have less-detailed explanations because they're already very well documented on the websites I reference in this chapter.

Creating Your Lab

The first step to creating your own lab is to select the cloud platform you will use to deploy your lab. This chapter will use the Azure platform to deploy the lab. However, for scenarios one and two, you can use your personal computer to perform the required tasks. Here are a couple of things to remember when reading these scenarios:

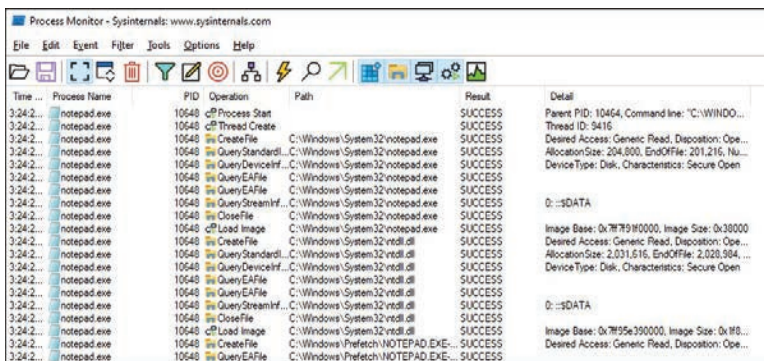
- If you already have experience performing the tasks for scenarios one and two, you can skip to scenario three.
- The explanation provided in this chapter won't go into deep technical details about each element covered in the scenarios. The intent here is for you to gain familiarity with the terminologies, gain some hands-on experience, and use it as a foundation to get started. You must be diligent and look for other sources of information regarding the technologies covered in each scenario. Some resources tailored to each scenario are available at *yuridiogenes.us*.

Scenario 1—Operating Systems Process

A deep understanding of operating systems is critical for any cybersecurity professional. You can access a curated list of online resources and books I recommend to

the process in the path shown in the **Path** column. To better understand this, do a simple test:

1. In the **Process Monitor**, click **Filter** and then click the **Filter** option.
2. Select **Process Name**.
3. In the name field, type **notepad.exe** and click the **Add** button.
4. Click the **OK** button.
5. Once the filtering is finished, click the Windows Start icon, type **notepad.exe**, and press **Enter**.
6. Now review the number of things that happened just by executing notepad.exe.
7. The **Process Monitor** window will be empty, and after you execute the previous step, you will notice the process and a thread being created, as shown in Figure 3.3.



Time ...	Process Name	PID	Operation	Path	Result	Detail
3:24:2...	notepad.exe	10648	Process Start		SUCCESS	Parent PID: 10464, Command line: "C:\WINDO...
3:24:2...	notepad.exe	10648	Thread Create		SUCCESS	Thread ID: 9416
3:24:2...	notepad.exe	10648	CreateFile	C:\Windows\System32\notepad.exe	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
3:24:2...	notepad.exe	10648	QueryStandard...	C:\Windows\System32\notepad.exe	SUCCESS	Allocation Size: 204,800, EndOfFile: 201,216, Nu...
3:24:2...	notepad.exe	10648	QueryDeviceInf...	C:\Windows\System32\notepad.exe	SUCCESS	Device Type: Disk, Characteristics: Secure Open
3:24:2...	notepad.exe	10648	QueryEaFile	C:\Windows\System32\notepad.exe	SUCCESS	
3:24:2...	notepad.exe	10648	QueryEaFile	C:\Windows\System32\notepad.exe	SUCCESS	
3:24:2...	notepad.exe	10648	QueryStreamInf...	C:\Windows\System32\notepad.exe	SUCCESS	D: ::\$DATA
3:24:2...	notepad.exe	10648	CloseFile	C:\Windows\System32\notepad.exe	SUCCESS	
3:24:2...	notepad.exe	10648	Load Image	C:\Windows\System32\notepad.dll	SUCCESS	Image Base: 0x7f79f0000, Image Size: 0x38000
3:24:2...	notepad.exe	10648	CreateFile	C:\Windows\System32\notdll.dll	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
3:24:2...	notepad.exe	10648	QueryStandard...	C:\Windows\System32\notdll.dll	SUCCESS	Allocation Size: 2,031,516, EndOfFile: 2,028,384, ...
3:24:2...	notepad.exe	10648	QueryDeviceInf...	C:\Windows\System32\notdll.dll	SUCCESS	Device Type: Disk, Characteristics: Secure Open
3:24:2...	notepad.exe	10648	QueryEaFile	C:\Windows\System32\notdll.dll	SUCCESS	
3:24:2...	notepad.exe	10648	QueryEaFile	C:\Windows\System32\notdll.dll	SUCCESS	
3:24:2...	notepad.exe	10648	QueryStreamInf...	C:\Windows\System32\notdll.dll	SUCCESS	D: ::\$DATA
3:24:2...	notepad.exe	10648	QueryStreamInf...	C:\Windows\System32\notdll.dll	SUCCESS	
3:24:2...	notepad.exe	10648	CloseFile	C:\Windows\System32\notdll.dll	SUCCESS	
3:24:2...	notepad.exe	10648	Load Image	C:\Windows\System32\notdll.dll	SUCCESS	Image Base: 0x7f95e390000, Image Size: 0x1f8...
3:24:2...	notepad.exe	10648	CreateFile	C:\Windows\Prefetch\NOTEPAD.EXE...	SUCCESS	Desired Access: Generic Read, Disposition: Ope...
3:24:2...	notepad.exe	10648	QueryEaFile	C:\Windows\Prefetch\NOTEPAD.EXE...	SUCCESS	

Figure 3.3 Events generated by executing *notepad.exe*

A process can create one or more threads, the basic unit the OS will use to allocate processor time. Why should you care about this information? Because when you are investigating a computer that is apparently compromised, you will use tools like Process Monitor to identify suspicious activities performed by a potentially malicious process.



Before moving to scenario 2, perform some extra tests. For example, in the **Process Monitor**, create a filter for *excel.exe*, open Microsoft Excel, type some formulas, and save the file in the *c:\temp* folder. Now go to

the **Process Monitor** and try to find the exact moment the file was saved. Right-click each operation and open its **Properties** to explore available information.



Note

You can learn more about processes and threads at <https://bit.ly/cybercareerch3link2>.



Note

Read this blog post to learn how Process Monitor can be used to investigate malicious activity: <https://bit.ly/cybercareerch3link3>.

Scenario 2—Network Traffic Analysis

Another foundational scenario you need to be familiar with is capturing and interpreting network traffic. Having a good understanding of how traffic flows between hosts is imperative for security professionals. While many tools are available to capture network traffic, the most common is Wireshark. This tool will enable your computer to listen to all network traffic and capture all frames for later analysis. Wireshark can also be used for network forensics and to identify malicious activities.



Note

An example of network forensics with Wireshark can be found at <https://bit.ly/cybercareerch3link4>. An example of malicious traffic analysis using Wireshark can be found at <https://bit.ly/cybercareerch3link5>.

You can perform the steps below on your home computer, just like in scenario 1. To get started with this experiment, make sure to download and install Wireshark from www.wireshark.org. After that, follow the steps below:

1. Open Wireshark.
2. On the first screen, you should see the available network interfaces. For example, you will see multiple options if you have an Ethernet connection (cable) connected to your computer and a WiFi connection. For

this example, we will select **Ethernet**. (This option requires a cable connection to your computer.)

3. Right-click **Ethernet** and then click **Start Capture**.
4. At this point, you should see a lot of traffic on the screen.
5. Open your browser and go to *www.pearson.com*.
6. Go back to Wireshark, click the **Capture** menu, and then click **Stop**.

Now that you have captured the traffic, let's make some sense of it. In a TCP/IP network, when you try to access a domain by providing the domain name, such as *www.pearson.com*, the next step is to identify who owns that domain (in other words, identify the IP address). To do that, your local computer will consult the Domain Name Service (DNS) to resolve that name. Using Wireshark, you can create a filter to see exactly when this happened. Type **dns.qry.name == "www.pearson.com"** to filter DNS queries for *www.pearson.com*, as shown in Figure 3.4, and then press **Enter**.

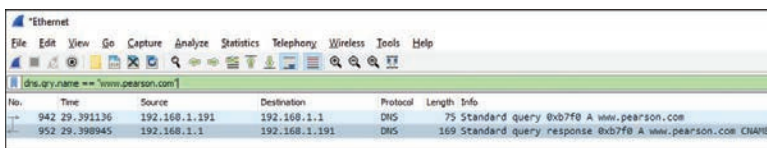


Figure 3.4 Creating filters in Wireshark

Notice that two packets appeared, one with the DNS query and the other with the DNS response. While the source and destination IP address from Figure 3.4 may vary according to your computer's network subnet, the point is that you were able to find exactly the moment that the name gets resolved. Now, let's see what a packet looks like. Click the first packet (DNS query), and you should see the different layers of information, as shown in Figure 3.5.

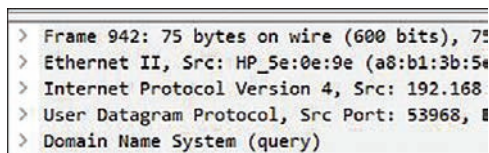


Figure 3.5 Reading a network package

These layers are explained below:

- The first layer on top contains information related to the frame itself.
- The second layer (Ethernet II) has the data-link layer, such as the computer's physical address, also known as Media Access Control (MAC) address. This address is unique for each network device.
- The third layer contains information about the network protocol in use, which in this case is the Internet Protocol (IP). Expanding this layer will show your computer's IP address and your DNS server's destination access.
- The fourth layer has information about the transport protocol in use, which, in this case, is the User Datagram Protocol (UDP). You will also find the source port (which will vary on each connection) and the destination port, which, in this case, is 53 (DNS service).
- The last layer contains information about the application, which, in this case, is DNS.

If you expand the transport and application layers, you should have a full visualization of the information you need for this exercise, as shown in Figure 3.6.

```

User Datagram Protocol, Src Port: 53968, Dst Port: 53
  Source Port: 53968
  Destination Port: 53
  Length: 41
  Checksum: 0x844b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 43]
  > [Timestamps]
  UDP payload (33 bytes)
Domain Name System (query)
  Transaction ID: 0xb7f0
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.pearson.com: type A, class IN
      Name: www.pearson.com
      [Name Length: 15]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 952]

```

Figure 3.6 Analyzing a DNS query

Repeat the same process for the second packet, the DNS response. In the response, you will see that the information is a bit different. Instead of having a section for queries, you will see a section for answers, as shown in Figure 3.7.

```
Domain Name System (response)
  Transaction ID: 0xb7f0
  > Flags: 0x0100 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  < Queries
    < www.pearson.com: type A, class IN
      Name: www.pearson.com
      [Name Length: 15]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  < Answers
    > www.pearson.com: type CNAME, class IN, cname wildcard.pearson.com.edgekey.net
    > wildcard.pearson.com.edgekey.net: type CNAME, class IN, cname e290.x.akamaiedge.net
    > e290.x.akamaiedge.net: type A, class IN, addr 173.222.216.14
  [Request In: 942]
  [Time: 0.007899000 seconds]
```

Figure 3.7 Analyzing the DNS answer

While this is a very simple analysis, it gives you an idea of the importance of understanding network traffic communication, protocols, and the use of Wireshark. New cybersecurity professionals who skip the foundational basics of computer networks have difficulty understanding how things work behind the scenes, impacting their capability to evolve in their field. For this reason, it is imperative to learn computer networks if you are going to work with cybersecurity.



Tip

Before moving to scenario 3, perform some extra tests. For example, clear the DNS filter, type **SSL**, and analyze the SSL traffic. Review the Client Hello and Server Hello packets.



Note

For more information about SSL handshake, see <https://bit.ly/cybercareerch3link6>.

Scenario 3—Cloud Security Posture Management

If you plan to work in cybersecurity, you must learn about cloud computing. Once you learn about cloud computing, you will quickly understand why one of the challenges organizations face nowadays is ensuring they have visibility and control over all workloads provisioned in their cloud environment. In addition, most attacks against cloud workloads are successfully accomplished because of customer misconfiguration, mismanagement, and mistakes. You need a cloud security posture management (CSPM) solution to ensure your cloud environment is more secure.



Note

Read this paper from NIST to learn the basics about Cloud Computing:
<https://bit.ly/cybercareerch3link7>.

Microsoft Defender for Cloud is the CSPM solution we will use in this scenario. Since this is a very mature product, there are many resources available that you can use to ramp up on this technology. The team that I manage at Microsoft created a Defender for Cloud Public Lab to help customers to learn more about the product, so for this scenario, follow the steps below:

1. Visit <https://aka.ms/MDFCLabs>.
2. Perform the steps from the following modules:
 - **Module 1:** In this module, you will provision your Azure environment using an Azure trial subscription.
 - **Module 2:** In this module, you will learn more about Defender for Cloud and how it helps to manage the security posture of your cloud environment.



Note

You can watch the *Defender for Cloud in the Field* show that I host to learn more about this product. Visit <https://aka.ms/MDFCInTheField> to watch all episodes.

After finishing these modules, you will have an environment ready for your 30 days trial. This means that now is the time to add the reminder on your calendar to ensure you cancel the subscription before the 30 days. Also, at this point, you must diligently perform all tests you need in this environment before the trial expires.

Scenario 4—Multi-Cloud Security

The “Flexera 2022 State of the Cloud Report” revealed that a multi-cloud approach is still the de facto standard among 89 percent of the organizations surveyed. This means you’re very likely to find a job in the cybersecurity field that requires you to know the main cloud providers—Microsoft (Azure), Amazon (AWS), and Google (GCP). Security posture management across multiple cloud providers can be even more challenging, and that’s why the CSPM solution must be able to provide visibility and control across clouds.

Defender for Cloud has this capability, and you can test it in the same lab environment that you started during scenario 3. To do that, go to <https://aka.ms/MDFCLabs> and complete modules 10 (GCP) and 11 (AWS). These modules will enable you to connect to each cloud provider and allow the information to flow to the Defender for Cloud dashboard.



Note

Read the “Flexera 2022 State of the Cloud Report” at <https://bit.ly/cybercareerch3link9>.

Scenario 5—Regulatory Compliance

As you look for cybersecurity jobs, you must be mindful of the industry you will be working in. For example, if you are going to be a cybersecurity analyst in a hospital (health industry), you might need to know the regulatory standards required for that industry. You don’t need to be an expert, but you should know what this means for the workloads you protect. Some of these workloads might need to comply with the Health Insurance Portability and Accountability Act (HIPAA).

The cloud security posture management platform needs to provide awareness of your workload’s security state. It needs to also provide security recommendations to help improve those workloads’ security posture by tailoring the hardening according to the industry standard, which, in this case, is HIPAA (Health Insurance Portability and Accountability Act of 1996).

To practice that, you will use the same lab from scenarios 3 and 4, but now you will follow the steps from Module 4.

Scenario 6—Attack Simulation

Many organizations adopt the red and blue teams strategy to better understand how threat actors operate and exploit vulnerabilities:

- **Red team** The red team is responsible for constantly attacking its own platform to identify breaches before the threat actors do it.
- **Blue team** The blue team is composed of defenders—cybersecurity professionals with relevant skills to ensure the environment is more secure. The blue team will also incorporate feedback from the red team to improve their security controls and reduce the likelihood of compromise.

If you are planning to work in this area within the cybersecurity field, this scenario is very important for you. Here are the labs you should perform to practice attack simulation:

- **Attack simulation for Windows** Visit <http://bit.ly/cybercareerch3link10> and follow the steps to execute attacks against a Windows system and see how Defender for Cloud detects those attacks. Notice that the attacker and target VMs can be provisioned in the same environment you created in scenario 3.
- **Attack simulation for Linux** Visit <https://bit.ly/cybercareerch3link11> and follow the steps to execute attacks against a Linux system. You can also provision the Linux VM in the same environment you created in scenario 3.

Scenario 7—Security Information and Event Management

Cybersecurity professionals who work on security operations (SOC) teams need to be familiar with the use of security information and event management (SIEM) systems. The goal of a SIEM solution is to aggregate data coming from different data sources, correlate this data, and enable security teams to consume this data for different purposes, including security investigation, incident response, and threat hunting.

Microsoft Sentinel is a cloud-based SIEM platform that operates on top of Azure but can ingest data coming from other cloud providers or on-premises resources. To practice hands-on activities in Microsoft Sentinel, visit <https://aka.ms/MSSentinelLab> and execute the steps from the following modules:

- **Module 1:** In this module, you will provision Microsoft Sentinel. You should use the Azure subscription trial you started in scenario 3.
- **Module 2:** In this module, you will start collecting data from different services.
- **Module 3:** In this module, you will create analytics rules and incidents.

- **Module 4:** In this module, you will learn more about incident management.

This is a long lab, so reserve enough time to perform it and review the terminologies you are unfamiliar with by visiting Microsoft Sentinel documentation at <http://aka.ms/SentinelDocs>.

Scenario 8—Threat Hunting

Threat hunting is a relatively new discipline that usually belongs to the security operations (SOC) team. Threat hunters usually perform a proactive investigation to identify indications of compromise (IOC) or indication of attack (IOA).

If you plan to work in the Security Operations Team, learning how to perform threat hunting is important. This expands your reach and adds an extra skill to your portfolio. Follow the steps below to practice different approaches for threat hunting (use the same Azure subscription that you used in previous scenarios for both tasks below):

1. Visit <https://aka.ms/MSSentinelLab> and execute the steps from Module 5.
2. This module will go over the steps on how to perform threat hunting using Microsoft Sentinel capabilities.
3. After you finish this module, visit <https://bit.ly/cybercareerch3link14> and execute the steps from there. This article will go over the steps to perform threat hunting using Defender for Cloud.



Note

Learn more about the different functions of a Security Operations Team at <https://bit.ly/cybercareerch3link12>. To learn the difference between IOC and IOA, visit <https://bit.ly/cybercareerch3link13>.

Scenario 9—Threat Intelligence

The use of threat intelligence has expanded over the years, and nowadays, most large organizations already understand that they must have this capability available. Threat intelligence gives context and actionable insights on attacks (active and old ones), as well as potential threats to the environment. This information is critical for decision-makers and security teams to use and be better prepared to deal with threat actors.

The MITRE ATT&CK® framework is “a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s attack life-cycle and the platforms they are known to target.” You can leverage this knowledge base to better understand how adversaries operate, which can be beneficial in many scenarios, including when you need to enrich your threat intelligence. Follow the steps below to learn how to navigate through the MITRE ATT&CK framework:

1. Visit the MITRE ATT&CK website at <https://attack.mitre.org>.
2. Click the **Search** button and type **ipconfig**. Wait until the results appear. Click the **ipconfig, Software S0100** link.
3. The **ipconfig** page supplies the details about this command, the mapping for the technique, and the groups (adversaries) used by this command. Notice that the technique in which this command is used is mapped to **System Network Configuration Discovery**.
4. Click this technique (**T1016**) to see that this is a subtechnique from **Discovery**. This means that in the discovery phase, the adversary is still trying to understand the environment. In other words, the threat actor is still at the beginning of their mission.
5. The MITRE ATT&CK framework is highly utilized in many products, including Microsoft Sentinel and Microsoft Defender for Cloud. To practice using threat intelligence in a SIEM platform, visit <https://aka.ms/MSSentinelLab> and complete the steps from Module 7.



Note

The definition for MITRE ATT&CK above is from the *MITRE ATT&CK: Design and Philosophy* ebook, which can be downloaded at <https://bit.ly/cybercareerch3link15>.



Tip

Before considering this scenario completed, spend more time navigating <https://attack.mitre.org>. For example, search for **Cobalt Strike**. When you open the Cobalt Strike page, look for **System Network Configuration Discovery** and then read the description about how Cobalt Strike uses this subtechnique.

Self-Assessment

I know this chapter has a lot of information to digest, and you must be tired by now. But, if you think about it, you just had a major tour across different

cybersecurity areas and the opportunity to practice many things and learn many new technologies.

Since this chapter was created using the 30-day Azure subscription, it is important for you to use at least 20 days to do all scenarios and have 9 days spare to review exercises that you have identified as needing more attention.

After you finish implementing all scenarios, reviewing all concepts, and taking notes, use Table 3.2 to perform a self-assessment per scenario. Notice that the entries in the **Completion** and **Observations** columns for scenarios 1 and 2 are only examples. The rest of the table is blank, so you can write your own observations.

Table 3.2 Self-assessment per scenario

Scenario	Completion	Observations
Understand operating system processes and threads	<i>100 percent</i>	I feel comfortable with this topic. Still need to dig more to understand threads, but I have a good idea of how things work.
Understanding the communication between two hosts in the same TCP/IP subnet	<i>90 percent</i>	I really liked this one. I feel like I can work all day long reading network packages. While I felt passionate about this topic, I still have a lot to learn because my background is not in computers. Need to do more computer network training.
Cloud Security Posture Management		
Multicloud Security Posture Management		
Understanding regulatory and compliance standards		
Simulating and detecting attacks on Windows and Linux		
Implementing a cloud-based Security information and event management (SIEM)		
Threat hunting		

Scenario	Completion	Observations
Gathering Threat Intelligence		
Understand operating system process and threads		
Understanding the communication between two hosts in the same TCP/IP subnet		

In Table 3.2, in the first two examples for the first two scenarios, the goal of the **Completion** column is to track how far you went on that scenario. Remember that while scenarios 1 and 2 are straightforward, others are more complex and will take longer. Ideally, you should finish everything, but you own your agenda, and if you don't have time to finish everything, the only requirement is to be honest with yourself and take notes to document your level of completion.

Another important column in this table is the **Observations**. The examples provided for scenarios 1 and 2 are some of the things that you can add. I advise you to write down which scenarios you were more excited and passionate about. This is when you will discover what triggers and motivates you and what you believe would be a good investment of your time to learn more. These nine scenarios cover different areas of cybersecurity, from the very basic level to the most advanced. Being exposed to all these tools and guided labs during the 30-day trial is an excellent way to identify which area you would like to work in the future.

1:1 WITH THE AUTHOR: BEING PASSIONATE IS AN IMPORTANT STEP FOR CAREER PROGRESS

Over the years, many professionals have reached out to me to ask how they could make progress in their careers. Some mistakenly assumed that because everyone was going one way, they also needed to go that direction. You can drive your career based on what is hot at the moment if that's what makes you happy.

Unfortunately, most people choose their direction based on money. I understand that being financially stable and well-compensated for your work is important, but it's not everything. You can earn a lot of money, but if you feel miserable at work, your life will be miserable. At some point, you will realize that the money was not worth it.

On June 12, 2005, during the Stanford University commencement address, Steve Jobs said: “The only way to be truly satisfied is to do what you believe is great work, and the only way to do great work is to love what you do. If you haven't found it yet, keep looking, and don't settle. As with all matters of the heart, you'll know when you find it. And like any great relationship, it just gets better and better as the years roll on. So keep looking, don't settle.”

This quote from Steve Jobs is perfect! It summarizes everything when it comes to a career. I hope you are migrating to cybersecurity because you feel passionate about it. And if you are not passionate yet, maybe all the scenarios you performed during this lab will give you something to think about and explore further.

I've seen many professionals who rose to the top because they were extremely passionate about what they did. At the same time, I've seen professionals change careers because they were not happy where they were. I remember talking to a friend who became a Judo Sensei after decades in the IT field. He told me that IT, for him, was a career that he liked, but he was never passionate about it. He was always passionate about martial arts, Judo in particular. He said that once he changed his career, he took a financial downgrade and had to readjust all his finances to break even. However, he said he was never happier, and his life changed completely. He doesn't regret the change. As a matter of fact, his only regret is that he didn't make the change earlier. He is still earning less money, but as I said earlier in this chapter, money isn't everything.

In summary: while there are plenty of opportunities in the cybersecurity field, you still need to decide your area of focus. Choose wisely when selecting where you will invest more time. Don't be driven only by the financial aspects, particularly if you are changing careers, as this is a great opportunity to reset and start over. Find your “why” and be passionate. If you do those things, your career will change for the better.

Summary

This chapter taught you how to create your cybersecurity lab based on nine scenarios. You learned about operating systems processes and threads, basic network communication, cloud security posture management, multicloud security, regulatory compliance, attack simulation, SIEM, threat hunting, and threat intelligence. In the next chapter, you will learn the importance of networking in the cybersecurity field, how to stay connected with the community, and how to leverage LinkedIn.

This page intentionally left blank

Numerics

20 *Coolest Careers in Cybersecurity*, 8–9

A

active listening, 133
adjusting your cybersecurity skills, 117–119
AI (artificial intelligence), 112
 ChatGPT, 144
 Microsoft Security Copilot, 145
 –related skills, 145–148
Amazon, hybrid work environment, 130
Angelou, M., 133
application security, 6
attacks, simulating in the lab, 57–58
automation, vulnerability assessment, 104
Azure Security Center in the Field, 135–136

B

Bezos, J., 119
bias
 confirmation, 116
 implicit, 115–116
 reducing, 116–117
big tech, cybersecurity jobs in, 19–20
Binary Defense, 158–159
“Bitwarden password vaults targeted in Google ads phishing attack”, 26
blogs, 52
 Rapid7’s impact by OpenSSL Buffer Overflow Vulnerability, 29
 Scripting Guy, 73
blue team, 7, 58
BSides, 66
buffer overflow, 29
burnout, 121
BYOD (bring your own device), 68, 73

C

calligraphy, 108
career/s. *See also* job/s
 being passionate about, 8, 22–23, 62–63, 154
 changing, 3–4, 47, 71
 cybersecurity, 4, 22
 job requirements, 9–12
 job titles, 8–10
 planning
 evaluating the options, 143–144
 explore your current skill, 26–30
 organizing your plan, 32–34
 self-assessment, 142–143
 SMART Goals, 30–32
 upcoming opportunities, 144–148
CC (Certified in Cybersecurity), 37
CCT (Certified Cybersecurity Technician), 41–42

- CEH (Certified Ethical Hacker), 39
- certification, 34
- CCT (Certified Cybersecurity Technician), 41–42
 - CISSP, 37
 - versus college degree, 35
 - CompTIA CySA+, 40–41
 - CompTIA Security+, 35, 38–39
 - Cyber and IT Security Foundation certification, 37–38
 - ECSS (EC-Council Certified Security Specialist), 39–40
 - ISACA (Information Systems Auditing & Control Association), 36
 - MCP (Microsoft Certified Professional), 35
 - specializations, 42–43
 - SSCP (Systems Security Certified Practitioner), 41
 - vendor-specific, 43–44
- changing careers, 3–4, 47
- chat, 131
- ChatGPT, 144
- cloud security
- architecture, 6
 - multi-, 57
 - posture management, 56
- coachability, 15
- Cobalt Strike, 46
- collaboration, 15–16, 107, 134
- commands, ipconfig, 60
- communication/communicating
- bad news, 107–108
 - influencing others, 132–133
 - remote worker, 131
 - skills, 39
- compliance, regulatory, 57
- CompTIA
- CySA+ certification, 40–41
 - Newsletter, 30
 - Security+ certification, 35, 38–39
- Conficker, 101
- confirmation bias, 116
- consulting, 152–153, 158
- continuing education, 157
- COVID-19 pandemic, 128, 135
- CQURE/CQURE Academy, 150, 153–154
- Cracking the PM Interview*, 21
- creative thinking, 107, 134–135
- critical thinking, 15
- CSO (chief security officer), 5
- curiosity, 155
- Cyber Seek Heatmap, 17–19
- cybersecurity, 4, 17–19
- analyst, 9
 - bias
 - confirmation*, 116
 - implicit*, 115–116
 - reducing*, 116–117
 - careers, 4
 - certification. *See* certification
 - consulting, 152–153, 158
 - diversity, 100–101
 - job/s, 8–12
 - basic qualifications*, 10
 - in big tech*, 19–20
 - marketing*, 21
 - product development*, 21
 - product engineering*, 21
 - product support*, 21
 - requirements*, 9–12
 - research*, 21
 - responsibilities and expectations*, 103–104
 - tenure*, 12
 - titles*, 8–10
 - obstacles, 112–114
 - penetration testing, 152
 - professionals, 100
 - roles and responsibilities, 5–8
 - running a business
 - common pitfalls and challenges*, 156–157
 - key elements for success*, 154–156
 - skills
 - adjusting*, 117–119
 - assessment*, 26–30
 - interviewing*, 11–12
 - soft*, 14–17
 - technical*, 12–14
 - specializations, 5–8, 42–43
 - terminology, 27
 - threat intelligence, 6
 - WLB (work-life balance). *See* WLB (work-life balance)
 - workforce gap, 4
- Cybersecurity Workforce Study 2022, 4
- ## D
- daily tasks, 124–125
- dashboards, 108
- data security, 6
- Deep Instinct, “Voice of SecOps Report 2022”, 112–113
- delegation, 16, 107
- DevOps, 6
- diet and exercise, 122
- Diogenes, Y.
 - Azure Security Center in the Field*, 135–136
 - Enterprise Mobility Suite Managing BYOD and Company-Owned Devices*, 73
- Overcome podcast, 112, 121
- Ready, Set, Achieve!: A Guide to Taking Charge of Your Life Creating Balance, and Achieving Your Goals*, 30, 120
- Windows Server 2012 Security from End to Edge and Beyond: Architecting, Designing, Planning, and Deploying Windows Server 2012 Security Solutions*, 72
- direct questions, 92
- directory services, 28
- discipline, 154
- discovery phase, threat intelligence, 60
- diversity, 100–101
- DMZ (demilitarized zone), 28
- DNS (Domain Name Service), query filter, 53

E

EC-Council University Cyber Talks, 67, 68–69
 ECSS (EC-Council Certified Security Specialist), 39–40
 email, 131
 empathy, 15, 133
 employer, treating as your customer, 106–108
From End to Edge and Beyond, 72
 endpoint security, 7
 enthusiasm, 87
 entrepreneur mindset, 106–108. *See also* success, key elements for
 ethical hacker, 100
 exercise, physical, 122
 Exin, Cyber and IT Security Foundation certification, 37–38

F

fear of failure, 140
 feedback
 employee, 133
 manager, 104
 soliciting, 133–134
 feelings
 gratitude, 114
 not taking things personally, 114–115
 stoicism, 113–114
 filter
 DNS query, 53
 job search, 80–81
 “Flexera 2022 State of the Cloud Report”, 57
 formal interview rounds, 88

G

Gaiman, N., 160
 Gilbert, J., *Enterprise Mobility Suite Managing BYOD and Company-Owned Devices*, 73
 Glassdoor.com, 19

Global Workplace Analytics, 128–129
 gratitude, 114
 growth mindset, 15

H

Hackers for Change, 70
 Heuer, R. J., *Psychology of Intelligence Analysis*, 116
 HIPAA (Health Insurance Portability and Accountability Act), 57
 Holiday, R., *The Obstacle Is the Way: The Timeless Art of Turning Trials into Triumph*, 112
 hybrid work, 130

I

IKE (Internet Key Exchange), 28
Ikigai, 140
 implicit bias, 115–116
 incident response, 120
 inclusivity, 15
 Information System Security Association International, 67
 infrastructure and endpoint security, 7
 interviewing, 11–12, 16–17, 66
 final decision, 93
 formal rounds, 88
 initial triage, 27
 interviewer angles, 88–89
 making a good impression, 86–87
 note-taking, 90
 power of enthusiasm, 87
 preparation, 85–87
 pre-triage process, 84
 questions, 90
 about previous experience, 92–93
 direct, 92
 fictitious scenario, 93
 scenario-based, 91
 technical, 88–89
 IP (Internet Protocol), 54
 ipconfig command, 60

IPsec, 28
 ISACA (Information Systems Auditing & Control Association), cybersecurity fundamentals certification, 36
 ISC2 (International Information System Security Certification Consortium)
 CISSP certification, 37
 SSCP certification, 41

J

Januszkiewicz, P., 150, 153–154
 job/s, 8–12, 27. *See also* interviewing; planning, career; remote work/er advancement/promotion, 119, 140, 142–143
 considerations, 141–142
 Ikigai, 140
 intermediate position, 143–144
 upcoming opportunities, 144–148
 competencies, 88
 cybersecurity
 basic qualifications, 10
 big tech, 19–20
 mapping your responsibilities, 104–105
 marketing, 21
 obstacles, 112–114
 product development, 21
 product engineering, 21
 product support, 21
 requirements, 9–12
 research, 21
 responsibilities and expectations, 103–104
 stress, 113
 tenure, 12
 titles, 8–12
 interviewing, 11–12, 16–17, 66. *See also* interviewing
 final decision, 93
 initial triage, 85
 making a good impression, 86–87

power of enthusiasm, 87
preparation, 85–87

pre-triage process, 84

lateral movement, 103

searching. *See also*

network/ing

Cyber Seek Heatmap,
17–19

LinkedIn, 79–81

phases, 94–95

progress timeline, 77–78

updating your resume,
78–79

Jobs, S., 8, 63, 108

Journal of Applied

Psychology, 8

K-L

Kennedy, D., 121, 151, 158–160

“Metasploit: The
Penetration Testers
Guide”, 152

lab

creating, 49

open-source, 46

operating systems process,
49–52

requirements, 46–49

scenarios

attack simulation, 57–58

cloud security posture
management, 56

multi-cloud security, 57

network traffic analysis,
52–55

regulatory compliance, 57

self-assessment, 60–62

SIEM (security
information and event
management), 58–59

threat hunting, 59

threat intelligence, 59–60

Windows Process

Monitor, 50–52

lateral movement, 103

leadership, 107

leveraging your skills,

108–109

LinkedIn, 9, 74–75, 79–81, 123

Linux, attack simulation, 58

listening, active, 133

M

MAC (Media Access Control)

address, 54

manager, feedback, 104

mapping your responsibilities,
104–105

marketing, 21

master's degree, 72–73

MCP (Microsoft Certified
Professional), 35

meetings, online, 131, 132

mental health, WLB (work-life
balance), 121, 123

Meta, 129

Microsoft Defender for Cloud,
56, 57, 135–136

Microsoft Outlook, tasks,
124–125

Microsoft Planner, 32–34

Microsoft Security Copilot, 145

Microsoft Sentinel, 58–59

Miller, J., *Ready, Set, Achieve!:*
A Guide to Taking Charge of
Your Life Creating Balance,
and Achieving Your
Goals, 30

mindset

entrepreneur, 106–108

of not taking things

personally, 114–115

MITRE ATT&CK

framework, 60

motivation, 154

multi-cloud security, 57

N

network/ing, 66. *See also*

interviewing

finding inward

opportunities, 70–71

online events and

communities, 67, 69–70

online presence, 73–74

LinkedIn, 74–75

Twitter, 76–77

security, 5

forensics, 52

traffic analysis, 52–55

VPN (*virtual private*
network), 27–28

security conferences,

66–67, 68–69

volunteering, 70, 71

newsletter, CompTIA, 30

NIST (National Institute of
Standards and Technology), 38

note-taking

interview, 90

post-deployment, 106

O

online events and

communities, 67

online meetings, 131, 132

online presence, 73–74

LinkedIn, 74–75

perception, 137

Twitter, 76–77

YouTube, 75–76

open-source lab, 46

operating systems

Linux, attack simulation, 58

Windows

attack simulation, 58

Process Monitor, 50–52

operational hygiene, 104

organizational structure, 102–103

Overcome podcast, 112

overthinking, 71

Ozkaya, E., 68

P

penetration testing, 152

physical exercise, 122

planning, career. *See also*

network/ing

evaluating the options,

143–144

explore your current skill,

26–30

Ikigai, 140

organizing your plan, 32–34

overthinking, 71

ramp-up phase, 105

self-assessment, 142–143

SMART Goals, 30–32

upcoming opportunities,

144–148

PoC (Proof of Concept), 106

podcasts

Overcome, 112, 121
We Hack Health, 121
 posture management, 7
 “The Potentially Large Effects of Artificial Intelligence on Economic Growth”, 144
 preparing for an interview, 85–87
 problem-solving skills, 133
 Process Monitor, 50–52
 processes, 50–51
 product development, 21
 product engineering, 21
 product management, 19
 product support, 21
 promotion
 considerations, 141–142
 Ikigai, 140
 self-assessment, 142–143
 PTES (Penetration Testing Execution Standard), 152

Q

questions, interview, 90
 about previous experience, 92–93
 direct, 92
 fictitious scenario, 93
 scenario-based, 91

R

ramp-up phase, 105
Rapid7's impact by OpenSSL Buffer Overflow Vulnerability, 29
 red team, 7, 58
 reducing bias, 116–117
 regulatory compliance, 57
 remote work/er, 128
 creativity, 134–135
 growth of, 128–129
 influencing others, 132–133
 online communication, 131
 soliciting feedback, 133–134
 time management, 135
 transparency, 136–137

report, lab scenario, 49
 requirements, lab, 46–49
 research, 21, 85–86
 responsibilities
 adjusting, 117–119
 cybersecurity job, 103–104
 mapping, 104–105
 resume, 11–12
 certification versus college degree, 35
 updating, 78–79
 Robertson, D., *How to Think Like a Roman Emperor: The Stoic Philosophy of Marcus Aurelius*, 112
 roles and responsibilities, cybersecurity, 5–8
 RTO (return-to-office)
 mandate, 130

S

scenario-based questions, 91
 scenarios, lab, 46–49
 attack simulation, 57–58
 cloud security posture management, 56
 multi-cloud security, 57
 network traffic analysis, 52–55
 operating systems process, 49–52
 regulatory compliance, 57
 self-assessment, 60–62
 SIEM (security information and event management), 58–59
 threat hunting, 59
 threat intelligence, 59–60
Scripting Guy blog, 73
 security conferences, 66–67
 self-assessment
 career advancement, 142–143
 lab, 60–62
 technical skills, 12–14
 Seneca, 113–114
 Senior Engineer–AI Security Engineer, 146

Shinder, T., *Windows Server 2012 Security from End to Edge and Beyond: Architecting, Designing, Planning, and Deploying Windows Server 2012 Security Solutions*, 72
 SIEM (security information and event management), 46, 58–59
 skills
 adjusting, 117–119
 AI-related, 145–148
 assessment, 26–30, 142–143
 communication, 39, 133
 critical thinking, 15
 interviewing, 11–12
 leveraging, 108–109
 mapping your responsibilities, 104–105
 organization, 154–155
 problem-solving, 133
 soft, 14–17, 84
 technical, 12–14, 84
 sleep, 123
 SMART Goals, 30–32, 114
 SOC (security operations center), 6, 59, 112
 soft skills, 14–17, 84
 specializations
 certification, 42–43
 cybersecurity, 5–8
 penetration testing, 152
 SSCP (Systems Security Certified Practitioner)
 certification, 41
 State of Remote Work 2020, 128
 stoicism, 112, 113–115
 stress, 113, 118–119, 135
 success, key elements for, 154, 159–160
 curiosity, 155
 discipline, 154
 facing challenges, 155
 giving back to the community, 155
 motivation, 154
 organization, 154–155
 teamwork, 156
 Swider, B., 86

T

tasks

- daily, 124–125
- plan-creation exercise, 105–106
- teams and teamwork
 - diversity, 100–101
 - lateral movement, 103
 - organizational structure, 102–103
 - success and, 156
 - virtual, 114
- technical skills, 12–14, 84
- technical writing, 72
- terminology, 27
- threads, 51
- threat hunting, 59
- threat intelligence, 6, 59–60
 - discovery phase, 60
 - MITRE ATT&CK framework, 60
- time management
 - daily tasks, 124–125
 - recommendations, 125
 - remote worker, 135
 - weekly goals, 124
- tools
 - communication, 131
 - Cyber Seek Heatmap, 17–19

- lab, 47–48
- Microsoft Planner, 32–34
- Wireshark, network traffic analysis, 52–55
- training, 157
- transparency, 136–137, 157
- TrustedSec, 121, 158
- tunnel vision, 120
- Twitter, 76–77, 151

U

- UDP (User Datagram Protocol), 54
- Uleman, J., 86
- unconscious bias, 115–116
- updating your resume, 78–79

V

- vendor-specific certification, 43–44
- virtual team, 114
- “Voice of SecOps Report 2022”, 112–113
- volunteering, 70, 71
- VPN (virtual private network), 27–28
- vulnerability assessment, 104

W

- We Hack Health* podcast, 121
- weekly goals, 124
- Windows
 - attack simulation, 58
 - Process Monitor, 50–52
- Wireshark, network traffic analysis, 52–55
- WLB (work-life balance), 119.
 - See also* time management
 - burnout, 121
 - diet and exercise, 122
 - establishing a baseline, 122
 - mental health, 123
 - promotion, 140–142
 - sleep, 123
 - time management, 124–125
 - tunnel vision, 120

X-Y-Z

- YouTube, 75–76
- Zuckerberg, M., 129