THE PEOPLE, PROCESS, AND TECHNOLOGY FOR OPERATING **SOC SERVICES**

THE MODERN SECURITY OPERATIONS CENTER

JOSEPH MUNIZ

FREE SAMPLE CHAPTER

The Modern Security Operations Center

This page intentionally left blank

The Modern Security Operations Center

The People, Process, and Technology for Operating SOC Services

Joseph Muniz

Addison-Wesley

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

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

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

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

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

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

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2021930517

ISBN-13: 978-0-13-561985-8
ISBN-10: 0-13-561985-8

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Acquisitions Editor
James Manly

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Ken Johnson

Proofreader
Betty Pessagno

Technical Reviewers
Anthony Giandomecino
Kevin Tigges
Willow Young

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Dedication

I would like to dedicate this book to two people. First, I want to dedicate it to Atticus Muniz, who can't walk, can't read, can't even understand how to use the toilet, but one day all of this will come. He is one year old and growing. Hopefully he will accomplish something great and while doing so make time to read this book. Second, I want to dedicate this book to Raylin Muniz, who is 11 and one of the most aggressive bookworms I've ever met. Hopefully she also will add this book to her reading list.

This page intentionally left blank

Table of Contents

Preface

Defending your organization from cyberthreats is a cat and mouse game. Both sides are constantly changing their tactics. When the defense tools work, the adversaries acquire the defense technology, reverse engineer it, and develop strategies to bypass it. When the adversaries start to succeed at bypassing security tools, defense companies take note, research the attack being used, and adjust defense capabilities in their tools to prevent future successful exploitation. Somewhere in between all of this back and forth is your organization.

Security is about the combination of people, process, and technology working together to accomplish a goal. You don't just buy a few products, plug them in, and magically eliminate the risk of being exploited. Security is a journey, which you must continue to invest in. It is not a destination. You don't one day become secure and be done with it. You can't buy your way to being secure. It requires an investment in a team responsible for security, commonly referred to as the security operations center (SOC).

Vision

My purpose for writing this book is to help every organization regardless of size, budget, or mission understand how to turn those responsible for the security of their organization into a security operations center. I do believe security is the responsibility of everybody in the organization, but one or more people need to have security as their primary job, and they need to be recognized for that role.

In this book, I describe how to build security services to support your organization. Some organizations run their business from the cloud. Other organizations do not. Some organizations have a budget to build a new SOC, while others need to convert what they have into a SOC that can support the organization now. Wherever you are at in your security journey, I have designed this book to incorporate industry guidelines, popular frameworks, and my own personal experience to give you an overview of how mature SOCs around the world run their security practice. I believe any organization can run a mature SOC as long as the organization recognizes its security team and what they do as a formal SOC.

My vision for this book is to take a vendor-agnostic approach to security with a focus on capabilities and best practices that will prepare you for the threats of tomorrow. I include tons of open-source and commercial product examples, but I always focus on the outcome of the recommendation so the vendor of choice won't matter. I reference specific guidelines to validate my recommendations and explain the risk of not performing what is covered in this book. I believe security professionals of all levels of experience can benefit from this book and I hope this book becomes a valuable asset in your journey against cyberthreats.

Who Should Read This Book?

I believe anybody with an interest in cybersecurity will benefit from this book. I explain concepts using different viewpoints ranging from what leadership expects to those behind the keyboard care about. Topics include building a SOC, risk management, vulnerability management, incident management, analysis of malware, compliance, digital forensics, situational and security awareness, and research and development. All of these topics correspond to services that are provided by mature SOCs around the world. Anybody who is interested in learning how to build these services into their security practice will benefit from this book.

How This Book Is Organized

This book can be used the day you start planning to build a SOC and can act as a resource to help mature an existing SOC. Chapter 1 starts with a general overview of all high-level SOC concepts. Chapter 2 focuses on how to build a SOC, including aligning the SOC to the business, mission statements, scope, and everything that should be considered as you plan a SOC.

Chapter 3 introduces the fundamental SOC services I find in mature SOCs around the world. I work through each service in the remaining chapters, including how to deal with risk, vulnerabilities, compliance, and other challenges organizations rely on the SOC to handle. Chapter 8 provides different approaches to some topics, such as when to launch an incident response versus a forensic investigation. Chapters 2 and 11 cover technologies that are common today as well as technologies that are futuristic but will eventually become part of the average SOC. An example is how cloud technologies such as Secure Access Service Edge (SASE) will eventually become as common as Voice over IP (VoIP) has become in most businesses.

Throughout this book I include examples of tools and techniques used by both red teams and blue teams, meaning I show how to execute real-world exploitation as well as how SOCs around the world defend against modern attacks. Many of the tools are open source, including using Kali Linux for exploitation, Ansible for automation, and NIST publications (among others) as guidelines. When the topic requires referencing enterprise tools, I try to bounce between vendors to give you a general feel of the capabilities rather than the specifics of how a particular vendor's tool functions. My goal is to keep a vendor-agnostic approach to security, which is why I include examples from many different vendors and open-source options.

Chapter 11 concludes this book by making predictions about the future of the SOC. My predictions are based on industry trends, conversations with customers, and personal experience in the industry for 20+ years. I believe many of the topics in this book are fundamental security concepts and will be relevant for many years after this book's publication. I wrote this to prepare you for the threats of tomorrow regardless of how they look. I believe this book has something for every organization to benefit from, and hope it helps you in your journey to building and running a successful security operations center.

Book Structure

I have organized this book from general SOC concepts to detailed SOC services. The following is a short summary of each chapter and how it relates to building and maintaining a mature SOC.

- **Chapter 1, "Introducing Security Operations and the SOC":** This chapter introduces high-level SOC concepts. I provide ways for you to validate which capabilities you currently have as well as how to assess your existing processes so you can plan where you can improve your SOC, if one already exists. The purpose of this chapter is to serve as a primer for the remaining chapters and help you establish your current state of security so you can use this book to develop a mature SOC.

- **Chapter 2, "Developing a Security Operations Center":** Chapter 2 focuses on the fundamental business and operational requirements that need to be in place before your SOC can provide service. Topics include who should sponsor, manage, and support the SOC, what type of policies and procedures need to be developed, and other business objectives that are essential prerequisites for your SOC goes live. The second half of this chapter focuses on operational requirements, such as how to plan the SOC workspace, how to accommodate SOC team members with different responsibilities, and what type of technology needs to be considered depending on what services your SOC plans to offer. Addressing the topics in this chapter is essential before your SOC can provide any value to the organization.
- **Chapter 3, "SOC Services":** This chapter introduces many of the topics that are explored in depth in the subsequent chapters of the book. I introduce the fundamental SOC services that are common in organizations around the world. I cover how these services can be delivered by the SOC and everything you need to consider as you look to stand up a new SOC service. This includes when you should outsource a service versus when it makes sense to develop the service using in-house capabilities. Chapter 3 represents the point at which your SOC is moving to a go-live state and starting to provide value to the organization.
- **Chapter 4, "People and Process":** Every SOC service requires the right people and processes to be successful. This chapter introduces all of the different job roles that are common in mature SOCs around the world. It describes skill requirements for each of the roles as well as expectations for daily duties. I cover how to find the right people for your SOC and groom them using different programs that tie directly back to the SOC's service success. Topics include job roles, recruiting, interviewing, onboarding, and outsourcing people and process.
- **Chapter 5, "Centralizing Data":** One fundamental SOC capability is being able to work with both the organization's data and external security data such as threat intelligence. Many new SOCs start off by offering log management and analysis services. This means the SOC is responsible for collecting logs from various tools, analyzing the logs, and providing a response when certain events are identified. Centralizing data is not an easy task as data comes in many formats and more advanced uses of data require different types of programming and automation skillsets. I cover everything related to how to collect and use data, which is a critical steppingstone to many of the other services offered in mature SOCs around the world.
- **Chapter 6, "Reducing Risk and Exceeding Compliance":** Dealing with risk and ensuring compliance are common requirements for many SOCs. The types of risk will vary between organizations, but in general, a SOC is responsible for reducing risk. Compliance can be mandated by local or federal government, mandated by service providers such as credit card companies, or mandated by an organization's leadership. In addition to these topics, this chapter

covers some peripheral topics because everything security related is a form of risk management and has some form of compliance element. For example, managing vulnerabilities can be part of a risk management program as well as a requirement to be compliant with some regulation or policy. I believe risk management and compliance are the most critical of the services your SOC can provide.

- **Chapter 7, "Threat Intelligence":** Building on Chapter 5, which stresses the importance of collecting and using data for SOC services, this chapter focuses on the critical data source of threat intelligence. I believe threat intelligence represents the future of all security technologies and thus have dedicated this chapter to the topic. Data is becoming too massive to manually review, and concepts such as baselining normal behavior or comparing things against what others are seeing is where the security industry is investing all developments. If your SOC is not leveraging threat intelligence today, it soon will be. If you are using threat intelligence, you will find in this chapter that there are many different ways to use threat intelligence, including looking beyond obtaining lists of things that are considered a high risk.
- **Chapter 8, "Threat Hunting and Incident Response":** One core service many organizations expect from the SOC is responding to incidents. This chapter covers how to develop a robust incident response service. Topics include how to plan a response based on the incident, how to contain, eradicate, and recover from an incident, when to use digital forensics, and what post-incident response activities should occur before you close out a case. Incident response is made up of many different services ranging from skillsets in analyzing malware to how to properly investigate an artifact without modifying it if legal action could occur. I include many tools and techniques so you can build a lab and eventually go live with a proper incident response capability.
- **Chapter 9, "Vulnerability Management":** Any SOC that is responsible for incident response should also include services for incident recovery and vulnerability management. By doing this, the SOC is able to reduce the risk of future security events based on the principle that an attack needs a vulnerability in order to succeed. Removing the vulnerability means the risk is reduced. This chapter focuses on vulnerability management services both from a proactive standpoint and a reactive standpoint. I believe if your SOC dedicates time to these topics, your organization will experience less attack behavior, leading to more time to focus on proactive services versus continuously reacting to security events.
- **Chapter 10, "Data Orchestration":** Many SOCs around the world have great data repositories and services but are finding their staff is being overwhelmed with tedious work. As a response to this problem, many organizations are investing in automation and orchestration with the goal of reducing mundane tasks and establishing a formalized and repeatable response to how they deliver SOC services. This chapter focuses on these topics, taking many of the concepts from previous chapters and looking at ways to apply orchestration and automation. Topics include tools, techniques, and programming, including an introduction to DevOps.

- **Chapter 11, "Future of the SOC":** This final chapter forecasts the future of the security operations center. I present a few industry trends that I believe will change the SOC of the future and explain how they look today as well as predict what they will look like in the future. Topics include Secure Access Service Edge (SASE), software-defined wide-area network (SD-WAN) technologies, general cloud trends, IT services, training, and the future of automation. I close this chapter and book with a focus on the future of your own SOC, a synopsis of how to take everything covered in this book and apply it to your SOC's journey to maturity and success.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Acknowledgments

I had a ton of help validating the content in this book and would like to recognize the reviewers, Anthony Giandomecino, Kevin Tigges, and Willow Young, for their hard work and valuable feedback. This book was a two-year journey to develop and these three kept me honest and the content on point. You will find this fine group of engineers have all spoken at industry events, have published various types of security content, and contribute to the security industry in many different ways. Hats off to them for helping me make this book project happen.

I would also like to thank James Manly and the rest of the Pearson team for their support during this long two-year journey from concept to publication. They are a very professional group and a pleasure to work with.

I would like to give a huge “thank you” to my friends and family for supporting me throughout this and my other projects. Also “thank you” to my managers at work and real boss, Anjelica Ruda, for allowing me to have time to work on this book in between all of the madness.

About the Author

Joseph Muniz is an architect and security researcher in the Cisco Security Sales and Engineering Organization. He is driven by making the world a safer place through education and adversary research. Joseph has extensive experience in designing security solutions and architectures as a trusted advisor for top Fortune 500 corporations and the U.S. government.

Joseph is a researcher and industry thought leader. He speaks regularly at international conferences, writes for technical magazines, and is involved with developing training for various industry certifications. He invented the fictitious character of Emily Williams to create awareness around social engineering. Joseph runs The Security Blogger website, a popular resource for security and product implementation. He is the author and contributor of several publications including titles ranging from security best practices to exploitation tactics.

When Joseph is not using technology, you can find him on the fútbol (soccer) field or raising the next generation of hackers, also known as his children. Follow Joseph at https://www.thesecurityblogger.com and @SecureBlogger.

Figure Credits

Cover image Sdecoret/Shutterstock

Figure 1-1, video posted by Anonymous on YouTube © 2020 Scripps Media, Inc

Figure 1-18, part of the MITRE ATT&CK matrix for Enterprise © 2015–2021, The MITRE Corporation

Figure 1-19, chaining together attack behavior using ATT&CK modeling © 2015–2021, The MITRE Corporation

Figure 2-5, Rapid7's Nexpose Vulnerability Scanner © Rapid7

Figure 2-6, Cisco Firepower passive vulnerability data © Cisco Systems

Figure 2-7, Cisco reputation block page © Cisco Systems

Figure 2-8, Google's reputation warning banner ©2020 Google

Figure 2-13, raised floor tile courtesy of Alibaba.com

Figure 2-14, sample SOC layout courtesy of Cisco Systems

Figure 2-26, Figure 5-16, SPLUNK Dashboard example © 2005–2020 Splunk, Inc

Figure 2-27, QRadar Dashboard example © IBM Corporation 1994, 2020

Figure 3-8, Tenable.sc vulnerability tracking © 2020 Tenable, Inc.

Figure 3-9, OpenVAS GUI example © Greenbone Networks 2020

Figure 3-11, MITRE ATT&CK Framework © 2015–2020, The MITRE Corporation

Figure 3-12, Atomic Red Ream website © 2014–2020 Red Canary

Figure 3-13, Atomic Red Team example for Windows © 2015–2020, The MITRE Corporation

Figure 3-14, Kali Linux Tool Categories © OffSec Services Limited 2020

Figure 3-15, searching Metasploit for Adobe vulnerabilities © Rapid7

Figure 3-20, Incident Response Consortium Playbooks © 2019 Incident Response Consortium

Figure 3-21, Malware Outbreak Playbook © 2019 Incident Response Consortium

Figure 3-22, diagram about hidden extensions © Microsoft 2020

Figure 3-24, Peframe analyzing a packed file © Microsoft 2020

Figure 3-26, using SET to clone Gmail © 2020 by TrustedSec

Figure 3-27, cloned Gmail website © 2020 Google

Figure 5-2, poorly parsed log within Splunk © 2005–2020 Splunk, Inc

Figure 5-3, Windows Event Log © Microsoft 2020

Figure 5-5, Splunk customized dashboard example © 2005–2020 Splunk, Inc

Figure 5-7, Splunk data input options © 2005–2020 Splunk, Inc

Figure 5-8, Cisco Stealthwatch configured to syslog data to Splunk © Cisco Systems

Figure 5-9, using default parsing template within SMC © Cisco Systems

Figure 5-10, results from poorly formatted Syslog © 2005–2020 Splunk, Inc

Figure 5-11, using custom syslog template in SMC © Cisco Systems

Figure 5-12, converting syslog data into reports and widgets © Cisco Systems

Figure 5-13, IBM QRadar search screen © IBM Corporation 1994, 2020

Figure 5-14, searching for data exfiltration in IBM QRadar © IBM Corporation 1994, 2020

Figure 5-15, IBM QRadar dashboard example © IBM Corporation 1994, 2020

Figure 5-17, Stealthwatch application within Splunk © 2005–2020 Splunk, Inc

Figure 5-18, IBM QRadar asset and vulnerability management example © IBM Corporation 1994, 2020

Figure 5-21, Firepower leveraging Rapid7 vulnerability data © Cisco Systems

Figure 5-25, Cisco Umbrella big data results example © Cisco Systems

Figure 6-1, Incident Response Consortium Playbook options © 2019 Incident Response Consortium

Figure 6-7, various Apache Struts exploits in Metasploit © 2020 The Apache Software Foundation

Figure 6-8, using Armitage to exploit a struts vulnerability © 2020 The Apache Software Foundation

Figure 7-2, Sophos threat prevalence usage example © 1997–2020 Sophos Ltd

Figure 7-3, example of Splunk not correctly processing threat data © 2005–2020 Splunk, Inc

Figure 7-5, Google Alerts example © 2020 Google

Figure 7-6, Google Chrome Scraper collecting hashes from the Cisco Talos blog © 2020 Cisco Systems, Inc

Figure 7-7, Twitter threat data behavior examples © 2020 Trend Micro Incorporated

Figure 8-2, Incident Response Consortium malware outbreak playbook example © 2019 Incident Response Consortium

Figure 8-4, opening a new incident ticket in Cisco SecureX © 2020 Cisco Systems, Inc

Figure 8-5, example of new case © 2020 Cisco Systems, Inc

Figure 8-7, Cisco AMP indicators of compromise example © 2020 Cisco Systems, Inc

Figure 8-8, hidden extension example © Microsoft 2020

Figure 8-10, TrIDNET Free File Analysis tool © Marco Pontello

Figure 8-17, Ghidra Disassembler viewing WannaCry ransomware kill switch © Lazarus Group

Figure 8-18, example of using Joe Sandbox for malware analysis © Lazarus Group

Figure 8-19, Cisco Stealthwatch identifying threats based on NetFlow © 2020 Cisco Systems, Inc

Figure 8-20, threat hunting maturity model © 2016–20 Sqrrl Fintech Private Limited

Figure 8-21, Cisco threat response analyzing success20.hopto.org © 2020 Cisco Systems, Inc

Figure 8-25, IRC Malware Outbreak playbook eradicate step © 2019 Incident Response Consortium

Figure 8-26, IRC Data Theft playbook eradicate step © 2019 Incident Response Consortium

Figure 8-27, IRC Malware Outbreak playbook recover step © 2019 Incident Response Consortium

Figure 8-29, Chain of Custody documentation bag example Courtesy of Cisco Systems

Figure 8-30, Autopsy main page © 2003–2020 Brian Carrier

Figure 8-31, Autopsy usage example © 2003–2020 Brian Carrier

Figure 8-40, Lessons Learned Meeting Agenda template example © Template.net

Figure 8-42, template for documenting parties involved © 2002–2020 Blackboard, Inc.

Figure 9-4, screenshot of Struts vulnerability example © 2020 Cisco Systems, Inc

Figure 9-5, screenshot of CVSS v2 base score calculator © National Institute of Standards and Technology

Figure 9-6, screenshot of CVSS temporal and environmental calculators © National Institute of Standards and Technology

Figure 9-7, screenshot of Struts CVSSv2 example © National Institute of Standards and Technology

Figure 9-8, screenshot of CVSS v3 base score metrics © National Institute of Standards and Technology

Figure 9-9, screenshot of Struts CVSS v3 example © National Institute of Standards and Technology

Figure 9-10, screenshot of Struts CVE-2017-9793 resource example © National Institute of Standards and Technology

Figure 9-11, screenshot of Struts vulnerability shown in Rapid7's Nexpose © Rapid7

Figure 9-12, screenshot of Rapid7 Nexpose dashboard © Rapid7

Figure 9-13, screenshot of passive vulnerability scanning example © 2020 Cisco Systems, Inc

Figure 9-14, screenshot of OpenVAS example © blackMORE Ops

Figure 9-17, screenshot of Certero dashboard example © 2007–2020 Certero

Figure 9-18, screenshot of network access control asset list example © 2020 Cisco Systems, Inc

Figure 9-19, screenshot of Zenmap © nmap.org

Figure 9-20, screenshot of Cisco Firepower tuning with vulnerability data © 2020 Cisco Systems, Inc

Figure 9-25, screenshot of Rapid7 Nexpose automated actions configuration example © Rapid7

Figure 9-26, screenshot of Nexpose Asset dashboard © Rapid7

Figure 9-28, screenshot of Cisco Firepower Apache Struts rules © 2020 Cisco Systems, Inc

Figure 10-2, screenshot of Splunk Phantom main dashboard example © 2005–2020 Splunk, Inc

Figure 10-3, screenshot of Splunk Phantom case management dashboard example © 2005–2020 Splunk, Inc

Figure 10-4, screenshot of Splunk Phantom Playbook template list example © 2005–2020 Splunk, Inc

Figure 10-5, screenshot of high-level Splunk Phantom Playbook example © 2005–2020 Splunk, Inc

Figure 10-6, screenshot of zoomed-in Phantom Playbook example © 2005–2020 Splunk, Inc

Figure 10-7, screenshot of phantom example of DevOps coding © 2005–2020 Splunk, Inc

Figure 10-8, screenshot of CrowdStrike Falcon dashboard example © 2020 CrowdStrike

Figure 10-9, screenshot of Falcon event graph example © 2020 CrowdStrike

Figure 10-10, screenshot of CrowdStrike Falcon example of event details © 2020 CrowdStrike

Figure 10-13, screenshot of IRC's Prepare playbook for malware outbreak © 2019 Incident Response Consortium

Figure 10-14, screenshot of IRC's Analyze playbook for malware outbreak © 2019 Incident Response Consortium

Figure 10-16, screenshot of Cisco ISE configured with Rapid7 Nexpose example © 2020 Cisco Systems, Inc

Figure 10-17, screenshot of Cisco Firepower configuration rule example © 2020 Cisco Systems, Inc

Figure 10-18, screenshot of Cisco SecureX orchestration example © 2020 Cisco Systems, Inc

Figure 10-19, screenshot of example workflow validation and run options © 2020 Cisco Systems, Inc

Figure 10-20, screenshot of Splunk Phantom workflow execution example © 2005–2020 Splunk, Inc

Figure 10-24, screenshot of new installation of MediaWiki © 2020 Cisco Systems, Inc

Figure 10-31, screenshot of Cisco Engineering and Software certification programs © 2020 Cisco Systems, Inc

Figure 10-32, screenshot of Cisco DevNet Sandbox Lab catalog of free labs © 2020 Cisco Systems, Inc

Figure 10-33, screenshot of Postman dashboard © 2020 Postman, Inc

Figure 10-34, screenshot of configuring Postman to communicate with a Cisco router © 2020 Postman, Inc

Figure 10-35, screenshot of configuration pulled into Postman example © 2020 Postman, Inc

Figure 11-5, Cisco SD-WAN dashboard example © 2020 Cisco Systems, Inc

Black and white portrait of fortune-teller with crystal ball © Aniriana/Shutterstock

Figure 11-9, article about the "Emily Williams" penetration test © 2020 Reed Exhibitions Ltd

Fortune Teller with Crystal ball © Pete Saloutos/Shutterstock

Figure 11-10, lab guide converted to Moodle © 2020 Cisco Systems, Inc

Figure 11-11, Khan Academy dashboard © 2020 Khan Academy

Woman fortuneteller with crystal ball in darkness © Konstantin Shevtsov/123rf.com

Seer working over glowing crystal ball © Phil McDonald/Shutterstock

Figure 11-22, Cisco DevNet Sandbox catalog of free DevOps labs © 2020 Cisco Systems, Inc

Chapter 4

People and Process

Never forget what you are. The rest of the world will not. Wear it like armor, and it can never be used to hurt you.

—"Tyrion Lannister," *Game of Thrones* (George R. R. Martin)

This chapter focuses on the human element of the SOC. These are the people that deliver the services covered in Chapter 3, "SOC Services," and will be the highest cost of running the SOC. According to a 2018 survey of 620 IT and cybersecurity professionals conducted by Enterprise Strategy Group (ESG), as summarized by Jon Oltsik, a senior principal analyst at ESG, "cybersecurity represents the biggest area where their [survey respondents] organizations have a problematic shortage of cybersecurity skills." This means not only are good people hard to find, they are even harder to keep because the technology industry has more jobs than people to run them. This chapter looks at what skills are recommended for different SOC job roles, how to recruit the right people, and strategies to keep those people excited to be part of your SOC. Without the proper people, process, and technology, your SOC will experience failures in services. Also, remember from Chapter 3 that people are one of the three pillars (along with work environment and technology) of the foundational SOC support services that must be in place before any SOC service can be launched. Let's now spend a chapter focusing on your people.

Career vs. Job

My mother used to explain that the difference between a job and a career is the perspective of the person doing the work—that is, how serious the person considers the work to be. For example, many teenagers look for a job simply to save enough money to purchase things they want. They don't care about advancements in their job because they are working just for the paycheck and typically don't even know or care about the mission of the organization they work for. By contrast, people who are career-driven are not showing up just for a paycheck. They also want career advancement, training to improve their skills, and the satisfaction of spending time working on something they enjoy doing.

The goal of this chapter is to help you not only plan to recruit career-driven people, but also develop and retain talent, because people are going to be your SOC's most important assets.

Developing Job Roles

Many different job roles fall under the categories "cybersecurity" and "information technology." Within those generic categories are roles that are responsible for presales, delivery of services, daily operations, and everything in between. Your SOC will have roles that fall under the cybersecurity and information technology categories; however, your SOC roles will require specific skills, knowledge, and experience based on the services your SOC offers. Sometimes skills, knowledge, and/or experience can be acquired on the job, while other times they are prerequisites for an employee to take on the associated responsibilities of a job role. Successful organizations clearly define job roles, compensation ranges, responsibilities, and paths for career growth because these elements are what attract and retain quality people.

In Chapter 1, I introduced the eight core services I find within mature SOCs. Each service has different types of job roles, which some can apply to multiple services while others are very specific to a single service. You will need to recruit and retain the right talent for the services you offer, which continues to be an extremely challenging task in today's competitive cybersecurity job market. Not only is it hard to find the right talent, but experienced talent will be expensive. You will have to decide when you can groom an internal employee for a role or seek external talent to fill a position.

One major factor that impacts these decisions is available budget for recruiting talent. Leadership will need a general number of what the cost will be to fill a SOC position. The best way to determine a ballpark cost to fill a SOC position will be using publicly available pay scales. The general schedule pay scale is an example of such a resource.

General Schedule Pay Scale

The U.S. federal government uses a scale based on series and grade to categorize and define jobs. The series is a numbered system for grouping similar occupations. For example, a computer engineer is part of the 0854 series, while a nurse is part of the 0610 series. The grade refers to the General Schedule (GS) pay scale representing the pay level for the job. A job role with a higher GS grade will have a higher pay range. Employees with a high school degree and little experience fall under the GS-5 and lower range, while people with work experience can expect to be at least at a GS-7 level. Employees with a master's degree and special experience will expect a GS-9 or higher job role. People looking to work for the U.S. federal government can use this system to quickly understand the pay range for any available U.S. federal job request. Candidates can also refer to the standardized language of the GS pay scale jobs to ask about how the existing role can advance to higher GS grades as the candidate gains experience in the role.

Note

The U.S. pay scale is just one example of a grade scale format. I believe the concept of grade scales is useful for better understanding a pay range and what is involved with a job. I believe grade scales more accurately represent the responsibilities of a job role than do job titles. In my experience, I've worked with people who have fabricated fancy job titles when their official title as documented within the organization is different. For example, a salesperson who is responsible for northeast sales might use the title Director of North East Sales even though he or she is not performing what the industry would consider director job duties. I've found that people who haven't had an increase in responsibility tend to eventually create their own made-up job titles. The most common example is using terms such as "Senior" to represent time served rather than an increase in responsibility. Time served does not automatically increase an employee's grade scale.

Formalizing Payscales

The GS pay scale is just one example of a pay scale you can use to standardize how compensation is distributed to each job role in your organization. You want to apply a formal pay scale to your SOC roles to set expectations for the pay range associated with your positions. You also need to be specific regarding what skills and other requirements are involved with each role to ensure potential candidates know what is required to qualify for the role. This also applies to advancements in a role. For example, as a SOC analyst gains experience, her title should change. A SOC analyst could start out as a grade 1 analyst. Once that analyst meets certain time, skill, and experience requirements, the analyst can request to be promoted to a grade 2, which will have a higher pay range. While skills are being obtained, salary increases should be provided that fall within the specific pay range. At some point, the candidate will hit the top of the pay range and must move to another pay range before any further increases in salary can be provided.

Formalizing pay scales enables employees to understand how their compensation will change as they increase in grade scale or switch roles, which will have their own assigned grade scale. Some job series will max out faster than others, encouraging an employee to switch roles if they desire a higher pay scale. An analyst series might max out at the role "analyst grade 5" while the pay for a analyst grade 5 is similar to a "architect grade 2" role. In this example, an analyst would not be able to make the same income as an architect grade 3 or higher, motivating the analyst to switch roles if he wants to be part of a higher pay scale than what an analyst pay scale could offer. Having certain job series max out at lower pay scales than other job series isn't a bad thing. Developing a job role structure with certain job pay scales maxing out lower than others encourages career development that is driven toward senior job titles. Companies that don't encourage career growth and just provide standard raises on an annual basis will not encourage employees to invest time into developing their skills or career. As a result, employees will remain unmotivated and a flight risk.

Note

Learn more about the GS pay scale at https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2019/general-schedule/.

IT Industry Job Roles

Job roles need to be clearly defined to identify a baseline of responsibilities as well as skills and experience expectations. The next section reviews the various types of jobs and their expected associated skills. It is up to your organization to customize and explain how the general skills associated with a job title relate to the specific job role and what additional skills and experience are desired for a potential candidate to be considered.

According to the employment website Indeed (https://www.indeed.com), the following items need to be included in a basic job title. Make sure to elicit responses to each of these categories with any job posting that you publish.

- **Job role:** Use targeted language rather than generic titles. Avoid lingo that is internally unique to your organization.
- **Job summary:** Sell your job with an attention-grabbing summary. Include the exact job location, including whether remote work is an option.
- **Responsibilities and duties:** Outline the core responsibilities. Highlight the day-to-day activities. Specify how the position fits within the organization and SOC.
- **Qualification and skills:** Provide a list of hard and soft skills. Keep the list concise.

To better understand job roles, let’s review common job titles and their associated skills.

Common IT Job Roles

Reviewing the common job roles that exist in the IT market space is a good place to start before focusing on the SOC-specific roles you will want in your organization. You can use the following list of IT industry job roles to better understand what type of skills are associated with a common IT title and determine if that role could apply to a SOC role you are looking to fill. Some roles will be tied to generating revenue, known as presales roles, while others will be supporting the organization in various fashions. Some job roles, such as a PCI DSS compliance officer, are tied to specific tasks, while others, such as a network engineer, are more generalized. The range and depth of skills will also vary between roles. A presales engineer might or might not have much hands-on experience with a technology depending on how the candidate utilized the technology in his or her previous role. It is best to qualify any skill during the interview process and validate experience through references.

Note

As you review these job roles, you might wonder how they relate to the SOC. As I've mentioned a few times in this book, the security industry is lacking sufficient qualified talent to fill all the jobs that are available. This concept holds especially true for people with SOC experience. I find that many organizations have to either grow SOC skills from within or expand their search to more generic IT skills in order to find available people. I will cover SOC job roles shortly, but it is extremely valuable to also know industry job titles as well. You might need to pull candidates from another IT field to find somebody for your SOC service.

- **Account manager (AM):** An account manager works in the sales and marketing department of a business and is responsible for managing client accounts. This job role requires very little technical knowledge, but it does require mature soft skills and a drive to execute on meeting or exceeding sales goals.
- **Sales engineer (SE):** A sales engineer combines technical knowledge with sales skills (a combination of hard and soft skills). Because many account managers lack technology knowledge, they require an engineer to handle technical-related tasks. Those tasks include understanding the customer's technical needs, explaining the technology or services those needs represent, providing demonstrations of technology, or possibly even installing technology to prove it can accomplish the desired goals so that a sale can be achieved. Sales engineers must be able to translate technical concepts into terms that nontechnical people understand.
- **Marketing engineer:** Organizations that sell products or services have teams dedicated to developing how those offerings are marketed to customers. Some marketing teams require creative people with a technical background to explain the value of the solutions being offered as well as validate if the marketing efforts meet their targeted customers' expectations. The level of technical and soft skills required for the marketing engineer position will depend on the type of products and services being offered as well as how the marketing engineer will be utilized.
- **Installation/post-sales engineer:** This role supports presales teams by delivering the products and services that were sold to the customer. Services could be short-term or long-term contracts and have various travel requirements. For example, an installation engineer could travel often to new customer locations for short projects or be part of a long-term deployment that spans across multiple locations.
- **Compliance officer:** Many organizations have compliance requirements that they must meet to offer certain types of services as well as to avoid the negative impact (such as fines) from not meeting mandatory compliance. Compliance officers are responsible for monitoring the current state of an organization's compliance status, obtaining proof that compliance is met, monitoring for changes in compliance, and performing other compliance-related tasks.

- **Manager:** Managers are responsible for addressing employees' needs. Fulfilling those needs can include operational requirements, such as providing tools and support to perform their jobs, or emotional support to encourage a positive working environment. Great managers help people achieve goals as well as mentor employees so they can grow their skills and feel accomplished. When employees experience challenges, managers are responsible for representing their needs. Managers are expected to have strong soft skills and experience managing people.

- **Desktop support:** The desktop support group focuses on managing host-related services. This can include support needed for desktops, laptops, mobile devices, and sometimes servers. Desktop support can be responsible for issuing equipment, enforcing security within equipment, and supporting the equipment with updates or software requested by employees. Desktop support can also develop policies for endpoints and support the SOC's mission of enforcing security policies. Skills can range between operating system types and tools, depending on experience level.

- **Helpdesk:** The helpdesk team is responsible for anything related to supporting employees and their equipment. This role is typically the first layer of support for an organization's internal services. Examples of common helpdesk job duties include resetting passwords, provisioning hardware and software, and responding to security incidents, such as a user reporting that her computer might be infected with a virus. The desktop support role and helpdesk role can be the same role or have responsibilities divided between different teams. A SOC can include a helpdesk service to assist with responding to security incidents and to support SOC team members' technical requirements.

- **Database/cloud engineer:** Organizations create data and need a place to store it. Data can be stored locally on servers or on a cloud storage service provider's servers. A database or cloud engineer acts as a data custodian ensuring that data is protected and policies created by the data owner are enforced. Technical skills include setting up relational databases, designing queries and reports to access information in the databases, and administering backup and recovery procedures.

- **Network engineer:** Network engineers deploy and manage the organization's networks. Every organization has some form of network services such as LAN, VPN, and wireless. Even organizations that lead with cloud services need a network to enable employees to access the cloud. Network engineer skills range from configuring to monitoring and troubleshooting various types of network equipment.

- **Software engineer:** Computer programs are computer code created by software engineers. As IoT and other technology grows in popularity, the need for programmability and applications increases the need for software engineers. Many SOCs leverage customized applications that are built by software engineers or leverage open-source tools that can leverage programmable tools that modify how the tool works or how the data is used by the tool. Software engineers develop information systems by designing, developing, and installing software solutions.

Note

A question I'm often asked is, "How do I start a career in cybersecurity?" My answer is that it depends on where you see yourself in three, five, and maybe even ten years from today. As the preceding list of the IT job roles indicates, many different types of work fall under the category "cybersecurity" or more broadly "information technology." Know that all the types of IT and cybersecurity job roles are not a good fit for you. There are many types of jobs within the world of IT that require different skills and personalities. I recommend identifying the type of work you want to do and speaking with people in that job role. As you consider a future career, factor in requirements for expected travel, work hours, compensation, required skills, and associated culture, even if some of these factors will be based on the specific employer offering the job. Once you find a desired job role, work toward education and experience specific to that role.

Some of the preceding job roles could apply to SOC work, while others do not but could perform SOC work with some level of training. I also didn't cover every job role you will find if you search popular job recruiting resources using terms like "cybersecurity" and "information technology" since the list could take up the entire chapter. Many of these jobs are also feeder roles into security-related work, meaning jobs people do before they start working in a SOC or undertaking similar security-related work. Sometimes people find a job in security later in their career because the candidate didn't initially pursue a career in security after completing their education, found an opportunity in non-security-related work prior to performing SOC work, wasn't qualified for security-related work, or other reasons.

SOC Job Roles

The expected career path for any job role in a SOC will depend on how the organization assigns responsibilities and pay scale to a job role. Roles in networking, software development, system engineering, and security intelligence can lead to entry-level SOC-related work. Entry-level SOC job roles such as junior analyst, consultant, or tester can lead to job titles such as senior architect or security administrator as responsibilities and pay scales increase. Know that there isn't a set standard for job roles or how roles feed into other roles, meaning the role of analyst at one organization could require the same experience as the role of architect at another organization. One organization might require specific certifications, degrees, or experience to meet the requirements of a job role, while the same job role at another organization will have different requirements. Consider industry and SOC job role, pay scales, and expected experience as you develop your strategy for recruiting for any job role in your SOC.

The job roles covered in the sections that follow make up common SOC-related career paths. These roles range from entry-level to senior-level job titles. The specifics of the work will depend on the type of service offered by the SOC. I will attempt to group similar job roles and explain skills based on what I have encountered in SOCs around the world. Use the recommended skills and certifications listed as reference points for what training and certifications you could pursue if you work in one of these job roles.

Note

I will follow up this section with an industry guideline for job roles known as the NICE Framework, which is much more detailed than my general list covered next. I will not list everything found in the NICE Framework but rather show you how to access and use that resource to research career path data.

Security Analyst

The security analyst role evaluates various types of data and plans and implements security measures to protect computer systems, networks, and data. Reviewing data can mean evaluating live network traffic or a copy of evidence such as event logs generated by security and network tools. In regard to a security operations center, a SOC analyst can be responsible for reviewing security logs and responding to events based on the services offered by the SOC. The skills associated with a security analyst can include reading logs and event data from various types of tools, implementing changes to security tools, such as configuring firewall rules, responding to incidents based on suspected events, and developing playbooks for the organization to standardize its responses to different events.

Table 4-1 outlines the responsibilities, skills, and certifications associated with the security analyst role. The security analyst role is ideal for the incident management SOC service but can also be part of the vulnerability management and research and development (R&D) services. Similar job titles include security engineer, security administrator, security specialist, and security consultant.

TABLE 4-1 Security Analyst Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Evaluate security measures and controls for vulnerabilities	Penetration and vulnerability testing, information security knowledge	CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester GPEN: GIAC Certified Penetration Teste CISM: Certified Information Security Manager
Establish plans and protocols to protect digital files and information systems against unauthorized access, modification, or destruction	Host security tools (antivirus, anti-malware, VPN), data loss prevention technologies, encryption concepts, identity management, access control	ECSA: EC-Council Certified Security Analyst Vendor NAC certification Vendor Data Loss certification Identity Management certification (e.g., Microsoft Active Directory)

Responsibilities	Skills	Certifications
Maintain data and monitor security access	TCP/IP, computer networking, routing and switching	GSEC: GIAC Security Essentials GCIH: GIAC Certified Incident Handler GCIA: GIAC Certified Intrusion Analyst CISM: Certified Information Security Manager
Perform security assessments and recommend security controls	Firewall and intrusion detection/prevention protocols	CISSP: Certified Information Systems Security Professional Vendor product certifications
Anticipate security alerts, incidents, and disasters and reduce their likelihood	Windows, UNIX, macOS, and Linux operating systems	Operating system certifications
Manage network and security systems	Network protocols and packet analysis tools. Windows, UNIX, macOS, and Linux operating systems	Vendor network certification (e.g., Cisco CCNA/CCNP/CCIE) Operating system certifications
Analyze security breaches to determine their root cause and impacted parties	Digital forensics and threat hunting	EC Council Computer Hacking Forensic Investigator certification
Recommend and install tools and countermeasures	Understand industry frameworks, security tools, and security process	ISC2 CISSP CompTIA CySA+
Provide training to employees in security awareness and procedures	Developing training programs	SANS Security Awareness Professional (SSAP)

Penetration Tester

The penetration tester role is focused on identifying vulnerabilities and testing those vulnerabilities in a similar manner to how an adversary would. Assessment officers and others that are responsible for identifying vulnerabilities tend to leverage automated tools and focus on identifying potential vulnerabilities but do not validate how realistic the vulnerability may or may not be. Penetration testers invest additional time validating that vulnerabilities exist using the same tools used by adversaries. Penetration testers attempt to exploit the vulnerability and then document the results. A penetration tester must be knowledgeable in how to identify vulnerabilities as well as common tactics used to exploit a vulnerability to achieve the same outcome a potential adversary could obtain. This skillset is commonly referred to as red team skills.

Table 4-2 outlines the responsibilities, skills, and certifications associated with the penetration tester role. A penetration tester is ideal for the vulnerability management SOC service but can also work in the compliance, risk management, and R&D services. Similar job titles include security analyst, security engineer, threat researcher, ethical hacker, red team member, and tester.

TABLE 4-2 Penetration Tester Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Perform penetration tests and assessments of web-based applications, networks, and computer systems	Exploitation, assessment, and audit skillsets; technical writing; legal and compliance understanding	CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester GPEN: GIAC Certified Penetration Tester
Conduct physical security assessments of servers, systems, and networks	Vulnerability and physical security assessment capabilities Lock picking	A+ and other hardware certifications
Design and create new tools and tests for penetration testing and assessments	Network servers, networking tools, security tools and products	OSCP and PEN-200 from offensive security CEPT: Certified Expert Penetration Tester
Probe targets and pinpoint methods that attackers could use to exploit weaknesses and logic flaws	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Employ social engineering to uncover security holes	Web-based applications and behavior science	OSCP: Offensive Security Certified Professional
Incorporate business goals into security strategies and policy development	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.)	CISSP: Certified Information Systems Security Professional CISM: Certified Information Security Manager
Research, document, and review security findings with management and IT teams	Vulnerability analysis and reverse engineering	CCFE: Certified Computer Forensics Examiner
Improve security services, including the continuous enhancement of existing methodology material and supporting assets	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.)	CISSP: Certified Information Systems Security Professional
Provide feedback, support, and verification as an organization fixes security issues.	Communication and writing	College degree

Assessment Officer

An assessment officer is responsible for identifying potential vulnerabilities or gaps in corporate policy, compliance requirements, or general security best practices as defined in popular frameworks. Unlike a penetration tester, an assessment officer works within specific scopes as defined by policies, compliance, or frameworks, meaning he or she must be aware of the latest requirements and continuously validate the organization is meeting those requirements. Any vulnerabilities out of scope of such requirements will be overlooked by the assessment officer because the focus of an assessment officer is auditing rather than general security validation. An assessment officer's skills are focused on business and operations with a strong understanding of industry frameworks, compliance, and laws associated with cybersecurity as it relates to the organization.

Table 4-3 outlines the responsibilities, skills, and certifications associated with the assessment officer role. An assessment officer is ideal for the compliance and risk management services but can also work in the vulnerability management service or assist other services such as incident management and R&D. Similar job titles are compliance officer, policy officer, security officer, and infosec officer.

TABLE 4-3 Assessment Officer Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Incorporate business goals into security strategies and policy development	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.)	CISSP: Certified Information Systems Security Professional CISM: Certified Information Security Manager
Conduct physical security assessments of servers, systems, and networks	Vulnerability and physical security assessment capabilities; lock picking	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Interview employees, obtain technical information, and assess audit results	Management and strong communication skills	College degree or special communication skills training CISM: Certified Information Security Manager
Understand industry data security regulations	Understand HIPAA, PCI DSS, etc.	Specific industry data security certification and experience
Develop and execute tests based on regulations being audited	Critical-thinking skills	College degree and/or programming certification
Research, document, and review security findings with management and IT teams	Critical-thinking skills	College degree and/or programming certification

Responsibilities	Skills	Certifications
Understand organization policies and procedures	Critical-thinking skills and experience with SOC policies and procedures	College degree
Provide feedback, support, and verification as an organization fixes security issues	Critical-thinking, project management, and communication skills	College degree

Incident Responder

An incident responder is a cyber first-responder or a higher-tier resource responsible for responding to a security incident. This role involves providing rapid initial response to IT security threats, incidents, and cyberattacks on the organization. The role can also include some penetration and vulnerability testing, network management, intrusion detection, security audits, network forensics, and maintenance of IT security systems. The primary responsibility may be monitoring traffic for any unusual activity or unauthorized access attempts and initiating the appropriate response when a potential event is identified. The response can include patching systems, initiating segmentation, isolating systems, alerting all associated parties, and assisting with returning impacted systems back to an operational state. The incident responder can work through the entire lifecycle of the incident or handle one part of the incident while higher-tier responders or other teams take over responsibilities, depending on the severity of the incident and how the SOC runs the incident management practice.

Table 4-4 outlines the responsibilities, skills, and certifications associated with the incident responder role. An incident responder is ideal for the incident management service but can also work in the situational and security awareness service or vulnerability management service. Similar job titles include incident response engineer, computer network defense, IT network defense, incident analyst, intrusion detection specialist, and network intrusion analyst.

TABLE 4-4 Incident Responder Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Actively monitor systems and networks for intrusions	Windows, UNIX, macOS, and Linux operating systems	Operating system certifications CompTIA CySA+
Identify security flaws and vulnerabilities	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester

Responsibilities	Skills	Certifications
Perform security audits, risk analysis, network forensics, and penetration testing	Exploitation, assessment and audit skillsets; technical writing; legal and compliance understanding; TCP/IP-based network communication	GCFE: GIAC Certified Forensic Examiner GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform desktop security assessments and update/patch potential vulnerabilities	Computer hardware and software systems; vulnerability assessments	GPEN: GIAC Certified Penetration Teste CEH: Certified Ethical Hacker
Develop a procedural set of responses to security problems	Operating system installation, patching, and configuration	CISSP: Certified Information Systems Security Professional CISM: Certified Information Security Manager
Establish protocols for communication within an organization and dealing with law enforcement during security incidents	Critical-thinking, project management, and communication skills	College degree
Create a program development plan that includes security gap assessments, policies, procedures, playbooks, training, and tabletop testing	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	CISSP: Certified Information Systems Security Professional College degree
Produce detailed incident reports and technical briefs for management, administrators, and end users	Critical-thinking, project management, and communication skills	College degree
Liaison with other cyberthreat analysis entities	Critical-thinking, project management, and communication skills	College degree
Handle case management duties of an incident and be involved with lessons-learned post-incident meetings	Case management experience and tools	CompTIA CySA+ CISM: Certified Information Security Manager College degree

Systems Analyst

A systems analyst is responsible for monitoring and interpreting different forms of data. Data can include logs from security tools, alerts from networking equipment, or other event data. A systems analyst might also be responsible for analyzing various types of artifacts, including files and programs, the goal being to determine whether there is any potential risk to the organization and discover the purpose of the artifact (meaning why it was created). For example, a word document might have a rootkit included, so the purpose of the document is to trick a user into running it and installing the rootkit.

Systems analysts that work in the incident management service spend time monitoring SIEM/SOAR/XDR systems, looking for potential threats within hundreds of thousands of event data points. A system analyst either addresses events directly or passes them to a member from the incident management service group. Systems analysts that work in the analysis service have isolated labs dedicated to containing potentially threating artifacts and learning what artifacts do. Common duties for analysts involved with the analysis service include performing static analysis, such as scanning or disassembling artifacts, and performing dynamic analysis, such as running artifacts in a sandbox to learn their behavior.

Table 4-5 outlines the responsibilities, skills, and certifications associated with the systems analyst role. A systems analyst is ideal for the analysis service or incident management service but can also work in the digital forensics and risk management services. Similar job titles include operations analyst, business systems analyst, business intelligence analyst, and data analyst.

TABLE 4-5 Systems Analyst Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Actively monitor systems and networks for intrusions	Windows, UNIX, macOS, and Linux operating systems	CCE: Certified Computer Examiner
Identify security flaws and vulnerabilities	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform security audits, risk analysis, network forensics, and penetration testing	Computer hardware and software systems; vulnerability management and exploitation tactics TCP/IP-based network communications	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform malware analysis and reverse engineering	Computer hardware and software systems	GCFA: GIAC Certified Forensic Analyst
Experience working with SIEM and SOAR orchestration and automation	DevOps and playbooks skills	Certification in DevOps

Responsibilities	Skills	Certifications
Reverse engineer/ disassemble malware and other artifacts	Disassemblers, debuggers, and other static-analysis tools	GIAC Reverse Engineering Malware (GREM)
Develop sandboxes and analyze software behavior	Sandboxes and other dynamic analysis tools	GIAC Reverse Engineering Malware (GREM)
Analyze logs and other data sources	Security tool logs (firewall, IDS/IPS, etc.), SIEMs, and SOAR	CCNA Cyber Ops, CompTIA Cybersecurity Analyst (CySA+)
Liaison with other cyberthreat analysis entities	Forensic software applications (e.g. EnCase, FTK, Helix, Cellebrite, XRY, etc.)	CREA: Certified Reverse Engineering Analyst
Understand assembly language and how computer systems operate (RAM, ROM, storage, etc.)	IDA Pro, Ghidra, RAM/ROM dumps	GIAC Reverse Engineering Malware (GREM)

Security Administrator

A security administrator is responsible for managing IT-related security and safety issues within a company. Tasks can include developing policies and procedures as well as overseeing that policies are followed by employees. Security administrators also oversee the implementation of solutions that prevent cyberthreats and protect data's confidentiality, integrity, and availability. Tasks include administering security controls to reduce the risk associated with potential vulnerabilities.

Table 4-6 outlines the responsibilities, skills, and certifications associated with the security administrator role. Security administrators are ideal for compliance, risk management, and situational and security awareness services. Similar job titles include security manager, information security manager, network security administrator, systems security administrator, information systems security officer, and IT security administrator.

TABLE 4-6 Security Administrator Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Protect systems against unauthorized access, modification, and/or destruction	Windows, UNIX, and Linux operating systems; system security capabilities	CompTIA Security+ (popular base-level security certification)
Perform vulnerability and networking scanning	Computer hardware and software systems; vulnerability management and exploitation tactics TCP/IP-based network communications	CCNA: Cisco Certified Network Associate CEH: Certified Ethical Hacker

Responsibilities	Skills	Certifications
Monitor network traffic for unusual or malicious activity	Strong understanding of firewall technologies	ECSA: EC-Council Certified Security Analyst CompTIA CySA+
Configure and support security tools such as firewalls, antivirus software, and patch management system	TCP/IP, computer networking, routing and switching	CISSP: Certified Information Systems Security Professional
Implement network security policies, application security, access control, and corporate data safeguards	Network protocols and packet analysis tools	CISM: Certified Information Security Manager CISSP: Certified Information Systems Security Professional
Train employees in security awareness and procedures	Critical-thinking, project management, and communication skills	College degree
Perform security audits and make policy recommendations	Intermediate to expert IDS/IPS knowledge; vulnerability evaluation; security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.).	CISSP: Certified Information Systems Security Professional College degree
Develop and update business continuity and disaster recovery protocols	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	College degree

Security Engineer

This role is similar to a security analyst, with responsibilities of performing security monitoring, security and data/log analysis, and forensic analysis. The goal of this role is to detect security incidents and launch a response. A security engineer can also have responsibilities for identifying which security technologies are used by an organization, maintenance of existing security technologies, development and maintenance of security policy, and developing methods to improve policies.

Table 4-7 outlines the responsibilities, skills, and certifications associated with the security engineer role. A security engineer can work in the incident management, analysis, digital forensics, and R&D services, depending on the specific skills and experience the engineer has acquired. Similar job titles include security analyst, security administrator, security architect, security specialist, and security consultant.

TABLE 4-7 Security Engineer Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Configure and install firewalls and intrusion detection/prevention systems	IDS/IPS, penetration testing, and vulnerability testing	CISM: Certified Information Security Manager CISSP: Certified Information Systems Security Professional CEH: Certified Ethical Hacker
Perform vulnerability testing, risk analyses, and security assessments	Firewall and intrusion detection/prevention protocols	CCNP Security: Cisco Certified Network Professional Security CEH: Certified Ethical Hacker
Develop or work with automation scripts to handle and track incidents	Secure coding practices, ethical hacking, and threat modeling	GSEC: Security Essentials GCIH: GIAC Certified Incident Handler GCIA: GIAC Certified Intrusion Analyst
Investigate intrusion incidents, conduct forensic investigations, and launch incident responses	Windows, UNIX, macOS, and Linux operating systems	CISSP: Certified Information Systems Security Professional CompTIA CySA+ CCFE: Certified Computer Forensics Examiner
Collaborate with colleagues on authentication, authorization, and encryption solutions	Critical-thinking, project management, and communication skills; encryption technology concepts	Systems Security Professional College degree
Evaluate new technologies and processes that enhance security capabilities	Critical-thinking, project management, and communication skills	College degree
Deliver technical reports and formal papers on test findings	Communication and technical writing skills	College degree
Supervise changes in software, hardware, facilities, telecommunications, and user needs	Critical-thinking, project management, and communication skills	College degree
Define, implement, and maintain corporate security policies	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	CISSP: Certified Information College degree
Analyze and advise on new security technologies and program conformance	Critical-thinking, project management, and communication skills	College degree
Recommend modifications in legal, technical, and regulatory areas that affect IT security	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	CISSP: Certified Information CISM: Certified Information Security Manager Systems Security Professional College degree

Security Trainer

A security trainer is responsible for implementing standardized training programs based on the organization's policies and the current threat landscape. Security trainers develop and schedule training needs based on feedback from interviewing leadership and employees. Responsibilities include developing the training material, coordinating and monitoring enrollment, schedules, costs, and equipment, and delivering training metrics to leadership. Other duties include researching industry training concepts, training people to deliver training content, and updating content as needed.

Table 4-8 outlines the responsibilities, skills, and certifications associated with the security trainer role. A security trainer is ideal for the situational and security awareness service but can also work in the risk management and R&D service groups. Similar job titles include training instructor, information assurance analyst, training analyst, security service training manager, and security training and development manager.

TABLE 4-8 Security Trainer Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Develop a schedule to assess training needs	Experience with technologies and best practices for instructional manuals and teaching platforms	Certification from talent and training associations
Ensure strict adherence to company philosophy/mission statement/sales goals	Understanding policies, procedures, and industry guidelines, standards, and frameworks	CISSP: Certified Information Systems Security Professional
Deliver training to customers or other trainers	Excellent verbal and written communication skills	College degree
Manage security awareness program based on threat research	Strong project management skills with the ability to supervise multiple projects	College degree
Deliver technical reports and formal papers on test findings	Identity and access management principles	College degree
Test and review created materials	Critical-thinking, project management, and communication skills	College degree
Maintain a database of all training materials	Basic database and program management skills	College degree

Security Architect

A security architect oversees the implementation of network and computer security for an organization. This role is typically a senior-level employee responsible for creating security structures, defenses, and responses to security incidents. Additional responsibilities may include providing technical guidance, assessing costs and risks, and establishing security policies and procedures for the organization.

Table 4-9 outlines the responsibilities, skills, and certifications associated with the security architect role. The security architect is ideal for the risk management service but can be part of other services such as compliance, situational, and security awareness, and research and development. Similar job titles include information security architect, IT security architect, and senior security analyst.

TABLE 4-9 Security Architect Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Plan, research, and design robust security architectures for any IT project	Risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies, and security attack concepts	CISSP: Certified Information Systems Security Professional
Perform vulnerability testing, risk analyses, and security assessments	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Research security standards, security systems, and authentication protocols	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	CISM: Certified Information Security Manager CISSP: Certified Information Systems Security Professional
Develop requirements for LANs, WANs, VPNs, routers, firewalls, and related network devices	Security controls such as firewall, IDS/IPS, network access control, and network segmentation	CISM: Certified Information Security Manager
Design public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures	Security and encryption technologies	CISM: Certified Information Security Manager EC-Council Certified Encryption Specialist (ECES)
Review and approve installation of firewall, VPN, routers, IDS/IPS scanning technologies, and servers	Security concepts related to DNS, routing, authentication, VPN, proxy services, and DDOS mitigation technologies	GSEC: GIAC Security Essentials GCIH: GIAC Certified Incident Handler GCIA: GIAC Certified Intrusion Analyst
Provide technical supervision for security team(s)	Critical-thinking and communication skills	College degree

Responsibilities	Skills	Certifications
Define, implement, and maintain corporate security policies and procedures	Network security architecture development and definition	CISSP: Certified Information Systems Security Professional College degree
Oversee security awareness programs and educational efforts	Critical-thinking and communication skills	College degree
Update and upgrade security systems as needed	Windows, UNIX, macOS, and Linux operating systems	A+ Security CISSP: Certified Information Systems Security Professional

Cryptographer/Cryptologist

A SOC that uses encryption to secure information or to build a system will assign these requirements to a cryptologist. A cryptologist researches and develops stronger encryption algorithms. A cryptologist may also be responsible for analyzing encrypted information from malicious software to determine the purpose and functions of the software.

Table 4-10 outlines the responsibilities, skills, and certifications associated with the cryptographer/cryptologist role. Cryptologists are ideal for digital forensics and analysis services but can work in other services based on the need for implementing, understanding, or identifying crypto.

TABLE 4-10 Cryptographer/Cryptologist Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Protect information from interception, copying, modification and/or deletion	Computer architecture, data structures, and algorithms	The cryptologist field is new and only has programs in universities and special learning programs. Certification programs include cryptology aspects, but dedicated certifications are not available at this point in time.
Evaluate, analyze, and target weaknesses in cryptographic security systems and algorithms	Linear/matrix algebra and/or discrete mathematics	EC-Council Certified Encryption Specialist (ECES)
Develop statistical and mathematical models to analyze data and solve security problems	Probability theory, information theory, complexity theory, and number theory	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification
Investigate, research, and test new cryptology theories and applications	Principles of symmetric cryptography and asymmetric cryptography	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification

Responsibilities	Skills	Certifications
Probe for weaknesses in communication lines	Principles of symmetric cryptography and asymmetric cryptography	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification
Ensure financial data is securely encrypted and accessible only to authorized users	Network Access Control concepts Data loss prevention technologies, encryption concepts, identity management, access control	Operating system certifications Vendor security certifications Authentication vendor certifications
Ensure message transmission data is not illegally accessed or altered in transit	Principles of symmetric cryptography and asymmetric cryptography	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification
Decode cryptic messages and coding systems for military, political, and/or law enforcement agencies	Principles of symmetric cryptography and asymmetric cryptography	EC Council Computer Hacking Forensic Investigator Certification College degree in math and cryptologist certification
Advise colleagues and research staff on cryptical/mathematical methods and applications	Principles of symmetric cryptography and asymmetric cryptography	College degree in math and cryptologist certification

Forensic Engineer

Many organizations will experience a breach, and they will need to understand how the breach occurred. Digital forensics is the art of collecting evidence regarding a security incident. Evidence can be used for legal actions, to remediate the vulnerability used to cause the breach, or as part of a lessons-learned exercise. Forensic engineers require specific skillsets focused on collecting data without creating changes to what they are collecting. These engineers may also have legal knowledge to assist with investigations that lead to legal actions.

Table 4-11 outlines the responsibilities, skills, and certifications associated with the forensics engineer role. This role is ideal for the digital forensics service but can also work in the analysis and incident management services. Similar job titles include forensic scientist, forensic consultant, and digital forensics engineer.

TABLE 4-11 Forensic Engineer Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Conduct data breach and security incident investigations	Network skills, including TCP/IP-based network communications	CCE: Certified Computer Examiner
Recover and examine data from computers and electronic storage devices	Windows, UNIX, and Linux operating systems	CEH: Certified Ethical Hacker
Dismantle and rebuild damaged systems to retrieve lost data	Windows, UNIX, macOS, and Linux operating systems; digital forensics concepts	EnCE: EnCase Certified Examiner
Identify systems/networks compromised by cyberattacks	Computer hardware and software systems	GCFE: GIAC Certified Forensic Examiner
Compile evidence for legal cases	Operating system installation, patching, and configuration	GCFA: GIAC Certified Forensic Analyst
Draft technical reports, write declarations, and prepare evidence for trial	Backup and archiving technologies; technical writing	GCIH: GIAC Certified Incident Handler
Give expert counsel to attorneys about electronic evidence in a case	Cryptography principles; legal experience; digital forensics experience; strong communication skills	CCFE: Certified Computer Forensics Examiner
Advise law enforcement on the credibility of acquired data	eDiscovery tools; strong communication skills	CPT: Certified Penetration Tester
Provide expert testimony at court proceedings	Forensic software applications (e.g. EnCase, FTK, Helix, Cellebrite, XRY, etc.)	CREA: Certified Reverse Engineering Analyst
Stay proficient in forensic, response, and reverse engineering	Data processing skills in electronic disclosure environments	CCFE: Certified Computer Forensics Examiner
		College degree

Chief Information Security Officer

Also called a CISO, this role is part of high-level management and is positioned as the person responsible for the entire information security division of an organization. A CISO is responsible for all assurance activities related to the availability, integrity, and confidentiality of customer, business partner, employee, and business information in compliance with the organization's information security policies. A CISO works with executive management to determine acceptable levels of risk for the organization.

Table 4-12 outlines the responsibilities, skills, and certifications associated with the CISO role. It is common for the CISO to be responsible for the risk management service but can also oversee all other SOC services.

TABLE 4-12 Chief Information Security Officer Responsibilities, Skills, and Certifications

Responsibilities	Skills	Certifications
Appoint and guide a team of IT security experts	Practices and methods of IT strategy, enterprise architecture, and security architecture	CISA: Certified Information Systems Auditor
Create strategic plan for the deployment of information security technologies and program enhancements	Security concepts; critical-thinking and communication skills	CISM: Certified Information Security Manager
Supervise development of corporate security policies, standards, and procedures	ISO 27002, ITIL, and COBIT frameworks	GSLC: GIAC Security Leadership College degree
Integrate IT systems development with security policies and information protection strategies	PCI DSS, HIPAA, NIST, GLBA, and SOX compliance assessments	CCISO: Certified Chief Information Security Officer
Collaborate with key stakeholders to establish an IT security risk management program	Network security architecture development and definition	CGEIT: Certified in the Governance of Enterprise IT
Anticipate new security threats and stay up to date with evolving infrastructures	Knowledge of third-party auditing and cloud risk assessment methodologies	CISSP: Certified Information Systems Security Professional
Develop strategies to handle security incidents and coordinate investigative activities	Critical-thinking and communication skills	CISSP-ISSMP: CISSP Information Systems Security Management Professional
Act as a focal point for IT security investigations	Critical-thinking and communication skills	CISSP: Certified Information Systems Security Professional College degree
Prioritize and allocate security resources correctly and efficiently	Critical-thinking and communication skills	College degree
Prepare financial forecasts for security operations and proper maintenance coverage for security assets	Critical-thinking and communication skills; contract experience	College degree
Work with senior management to ensure IT security protection policies are being implemented, reviewed, maintained, and governed effectively	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	College degree

Every job role you recruit for will have an associated learning curve to onboard an employee into your SOC environment. Every SOC has its own unique networks, processes, and capabilities that can only be taught while in the job role. The next section looks at role tiers to better understand how job titles can change as employees gain experience and knowledge.

I opened this section with the caveat that a wide variety of different names are used for similar job roles. What you believe a security analyst does, for example, may be different from what others think that job role entails. To help standardize job role concepts, next I'll cover a U.S. government guide regarding responsibilities associated with cybersecurity industry jobs.

NICE Cybersecurity Workforce Framework

The previous section defined SOC roles found in SOCs around the world. Another approach (among many) to exploring these roles and alternative names for them is the U.S. government resource known as the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework). I include this reference as an alternative to how I see job roles within the SOC, since different people will interpret job titles differently.

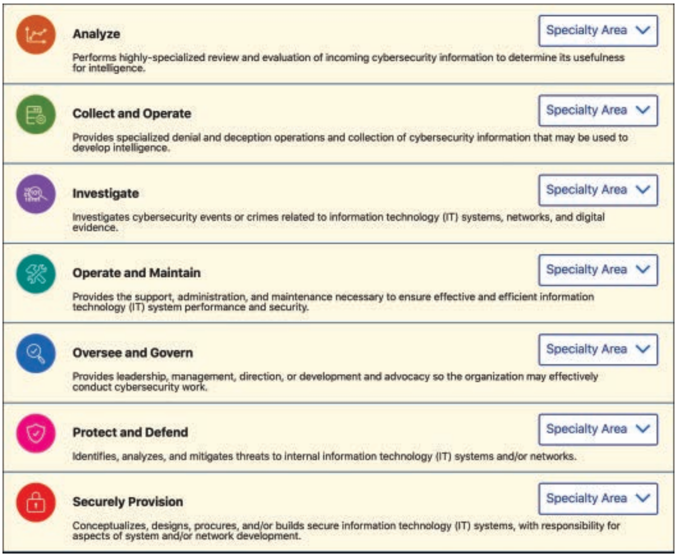
The NICE Framework is part of the Cybersecurity and Infrastructure Security Agency's National Initiative for Cybersecurity Careers and Studies (NICCS) and is described on the NICCS website as "a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed." You can use the NICE Framework to develop job requirements for recruiting, to prepare questions for interviewing potential candidates, and to get an idea of the skills associated with common cybersecurity job tiles. The rest of this section describes how to drill down to specific job roles on the NICE Framework web page at https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework.

Nice Framework Components

The NICE Framework is composed of the following components:

- Seven categories representing a high-level grouping of common cybersecurity functions
- Thirty-three Specialty Areas representing distinct areas of cybersecurity work
- Fifty-two Work Roles representing the most detailed groupings of cybersecurity work and composed of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role

Figure 4-1 shows the seven categories of the NICE Framework as presented on the NICSS website. Notice that the description for each category focuses on the type of work from a high level regarding the type of skillsets people have that work within the category's field of focus. The descriptions are developed this way to accommodate multiple specific skillsets that may fall under a more generic category. For example, suppose I need an analyst for my incident management SOC service and I want to identify specific job requirements for purposes of recruiting an analyst. I would start with the Protect and Defend category based on the description "Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or network" that indicates people in this category have skills in evaluating and responding to events based on security logs or other event logs, which is what incident management is all about. Categories are outcome focused, meaning the field of work, so I would need to drill down deeper to identify associated job roles.



Analyze

Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Investigate

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

Protect and Defend

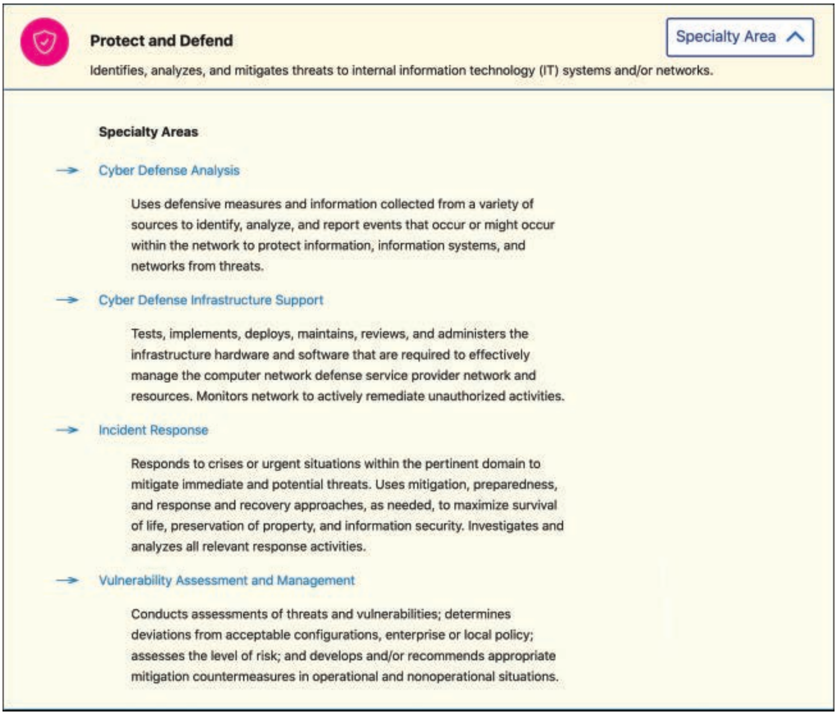
Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

Securely Provision

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

FIGURE 4-1 NICE Framework Seven Categories

To better understand the job skills in the Protect and Defend category, I can click the category's Specialty Area button. Figure 4-2 shows the Protect and Defend category and its four Specialty Areas. Because I am looking for a description of the skills of an analyst for my incident management service, I can narrow down the Specialty Areas to two of the four based on their descriptions: Cyber Defense Analysis and Incident Response. I believe the Vulnerability Assessment and Management Specialty Area could also be useful but would be more relevant to the vulnerability management service than the incident management service for which I need to recruit an analyst. The Incident Response role would be the best choice, but the Cyber Defense Analysis could also do the job based on the number of similar skills as seen with an Incident Response job role. In order to see the specific skills associated with a job role, I will need to click into that role.



Protect and Defend

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

Specialty Areas

→ Cyber Defense Analysis

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.

→ Cyber Defense Infrastructure Support

Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

→ Incident Response

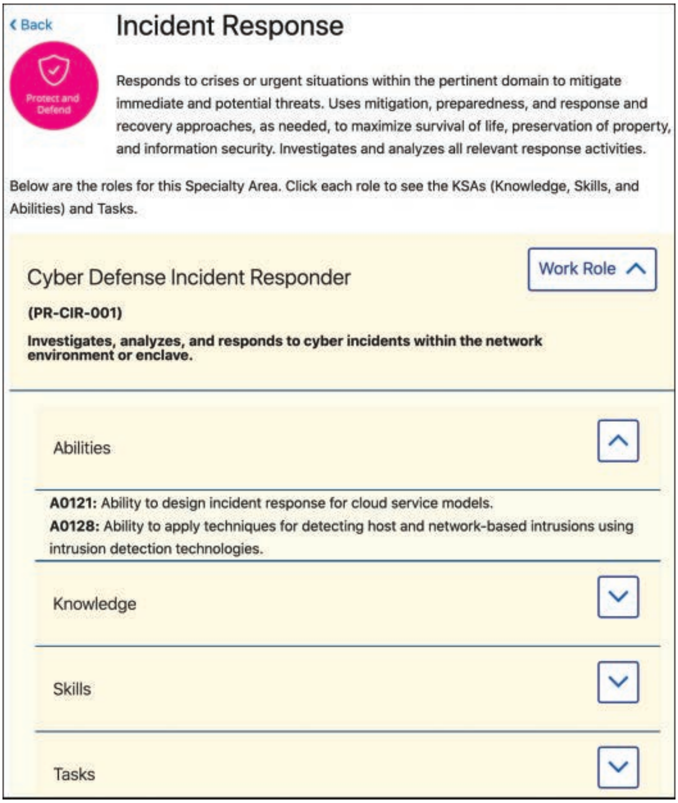
Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

→ Vulnerability Assessment and Management

Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

FIGURE 4-2 NICE Framework Protect and Defend Category with Four Specialty Areas

Next, I'll go with my first pick, which is Incident Response specialty area. To see the details of a specialty area, I click the specialty area to bring up the Work Role details. Figure 4-3 shows some of the details of the Cyber Defense Incident Responder Work Role, including a description of the role and the required abilities. As Figure 4-3 indicates, details regarding the knowledge, skills, and tasks of a Cyber Defense Incident Responder can be displayed by clicking the drop-down arrows. The language used by NICE to explain the job role is much more specific, allowing a better understanding of what tasks this type of employee would be expected to know how to do.



Incident Response

Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Below are the roles for this Specialty Area. Click each role to see the KSAs (Knowledge, Skills, and Abilities) and Tasks.

Cyber Defense Incident Responder

(PR-CIR-001)

Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Abilities

A0121: Ability to design incident response for cloud service models.
A0128: Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

Knowledge

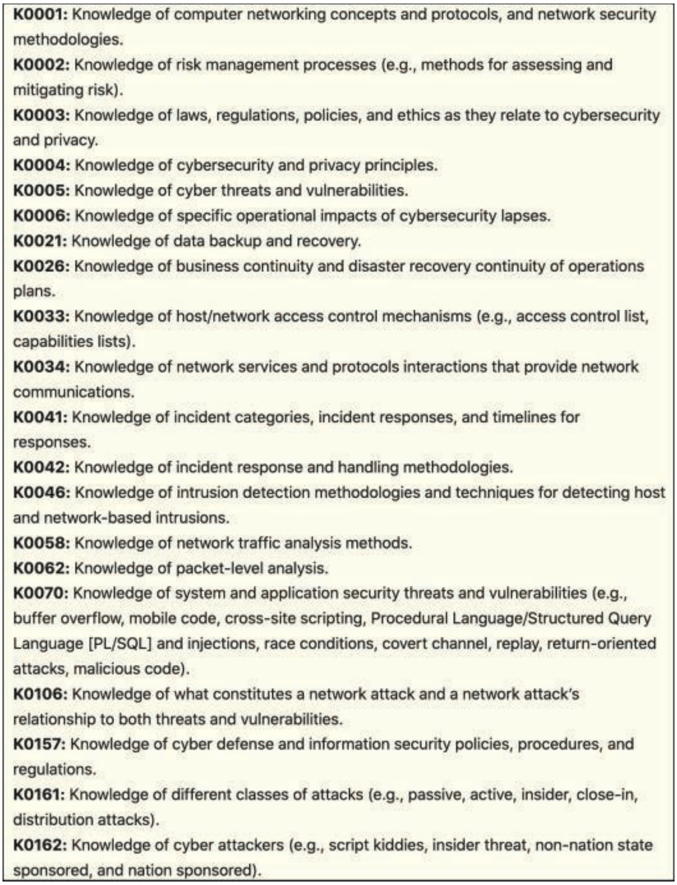
Skills

Tasks

FIGURE 4-3 NICE Framework Cyber Defense Incident Responder Work Role Details

Clicking the Knowledge tab in the Incident Responder job role reveals tons of knowledge concepts, as shown in Figure 4-4. These concepts can be extremely useful when creating a job profile for the candidate you plan to recruit for. In Chapter 3, I pointed out that many SOC managers who are responsible for starting a new SOC service don't know what skills they will need until the service goes live, making it challenging to develop a job profile for a service before it exists. Using the NICE Framework not only can help you develop requirements for job roles based on industry trends but also provides you with a validation point for the type of job titles you should seek out based on what the NICE Framework lists as expected skills associated with a job title.

I highly recommend using the NICE Framework if you don't know the type of skills a person needs to have to work for your SOC service. This same concept can apply as you develop interview questions for potential candidates.



K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004: Knowledge of cybersecurity and privacy principles.
K0005: Knowledge of cyber threats and vulnerabilities.
K0006: Knowledge of specific operational impacts of cybersecurity lapses.
K0021: Knowledge of data backup and recovery.
K0026: Knowledge of business continuity and disaster recovery continuity of operations plans.
K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K0034: Knowledge of network services and protocols interactions that provide network communications.
K0041: Knowledge of incident categories, incident responses, and timelines for responses.
K0042: Knowledge of incident response and handling methodologies.
K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0058: Knowledge of network traffic analysis methods.
K0062: Knowledge of packet-level analysis.
K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0157: Knowledge of cyber defense and information security policies, procedures, and regulations.
K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0162: Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).

FIGURE 4-4 NICE Framework Cyber Defense Incident Responder Knowledge Tab Details

Role Tiers

Roles within each SOC service can be broken down into different tiers or skill levels, which signify associated responsibilities. For example, a first-tier SOC analyst may be responsible for detecting, identifying, and troubleshooting security events that come into the SOC. Often this is the tier that communicates with the affected party. Responsibilities include detection, classification, and escalation of events. A second-tier analyst may have mitigation responsibilities over any event escalated by a first-tier SOC analyst. If the event requires even further support, a more-experienced third-tier analyst may be involved to remediate the situation. The third-tier analyst might also build tools and processes to improve capabilities within the SOC, including the processes followed by lower-tier analysts. Higher-tier roles have higher compensation but require deeper technical skills and experience. The same tiered approach can apply to other job roles with SOC services, such as a first-tier developer handling basic coding while a higher-tier developer would have responsibilities over the project's direction.

Each job role you create for your SOC should have a tier structure to promote career growth. A pay scale should also be assigned to each tier of a job role to inform employees what the expected compensation range is with an associated job role. The specific requirements advertised for the job role that includes the associated tier can reference lower tiers along with including the additional experience and skills needed to be considered for the higher-tier job role. Using this structure not only weeds out candidates that do not have the associated skills for the job tier being requested but opens the door for those same candidates to consider a lower tier of the same job role that might be more appropriate for their skill and experience level. For example, a SOC might post open job roles for multiple analyst jobs at different tier levels. A candidate who interviews for the tier 3 analyst role might be informed that he is not qualified for that role but should consider applying for a tier 1 or 2 analyst role, with the goal of eventually gaining the experience to be promoted to a tier 3 analyst. Using this approach will provide direction for career growth, open your recruiting efforts to more candidates, and keep expectations for hiring and promotions clear to all employees.

It is important to validate industry pay ranges and experience expectations against any job role you create as well as the tier you associate the role with. With publicly available sources of pay ranges online, job candidates have expected pay ranges for specific job titles. The same expectation applies to associated tiers with a job title. For example, job and recruiting website Glassdoor estimates an average base pay for a tier 1 analyst at $77,665 per year USD, while an experienced analyst salary range increases to $99,898 per year USD. Aligning with industry trends for pay ranges will reduce the risk of not capturing quality candidates as a result of not advertising acceptable pay scales in your job posting. You should apply similar research to expectations for skills and experience. Online employment resources such as Glassdoor and Monster not only provide expected pay ranges for job roles, but also suggest years of experience in the role and a generic view of expected skills. Use these expectations as you list out what requirements for skills and experience are needed for your job roles, keeping in mind that your job roles will be based on the services provided by your SOC and will be different than a generic industry explanation of a job title and associated experience tier.

Note

Other factors, such as geographical considerations, can impact the salary for a job role. For example, a candidate for a job in San Francisco will expect a much higher salary than a tier 1 analyst candidate in Des Moines.

SOC Services and Associated Job Roles

The roles and job skill requirements for your SOC will depend on the different services the SOC is responsible to deliver to its customers. People are required for any SOC service regardless of the type of technology being used. Even the value from advanced security analytics such as artificial intelligence boils down to how the SOC uses the technology. Software does not provide the answers to what problems your SOC faces; it provides the tools and delivers the data needed to discover answers. Essentially, people are needed to run technology and to interpret the results of the tools used in the SOC.

The following sections review how people relate to the different services that can be offered by a SOC. Each service will be made up of one or more job roles previously described in the chapter.

Risk Management Service

The risk management service is responsible for managing all aspects of risk to the organization. This includes analyzing risk, calculating the potential impact of risk, and making decisions based on the organization's risk appetite. Employees responsible for risk management must have great communication skills, enabling them not only to ensure that everybody in the organization understands any significant risk but also to explain the organization's risk management strategy. Working for the risk management service also requires a solid understanding of business, because decisions of the service will impact various internal and external elements of the organization. Successful employees responsible for risk management are skilled at negotiation and diplomacy. They can work under pressure and are able to modify strategies as various factors change the current state of the organization's risk status.

Possible job titles include chief information manager, chief information security officer, security officer, risk management analyst, and analyst.

Vulnerability Management Service

Successful employees responsible for vulnerability management have experience in and understanding of network and computer security. They can analyze hardware, software, networks, and communication to discover and address vulnerabilities. SOC members involved with vulnerability management have solid communication skills so they can explain identified vulnerabilities as well as work with various parties to validate findings, including third-party vendors and other external experts. Employees responsible for vulnerability management are detail-oriented, have strong problem-solving skills, and can adapt methods used to manage vulnerabilities based on the ever-changing threat landscape.

Possible job titles include penetration tester, vulnerability engineer, ethical hacker, red team tester, security analyst, and security engineer.

Incident Management Service

SOC employees responsible for incident management actively monitor systems and networks for intrusions. The incident management team develops a procedural set of responses to security problems and oversees their execution. This team is also responsible for restoring services back to a normal state following an incident as quickly as possible while minimizing the impact to business operations. Communication and diplomacy skills are required to produce incident reports and provide technical briefings to various parties about incidents in a diplomatic fashion. Employees are required to be able to work under pressure while coordinating all activities required to perform, monitor, and report on the incident management process.

Possible job titles include incident responder, security analyst, computer network defense, IT network defense, incident analyst, intrusion detection specialist, and network intrusion analyst.

Analysis Service

A security analyst is responsible for detecting and preventing cyberthreats to an organization. Members of the analysis team review security logs from various types of devices and work with the team responsible for incident management when a threat is confirmed. In addition to dealing with real-time threats, the analysis team analyzes and responds to undisclosed hardware and software vulnerabilities when a dedicated vulnerability management team isn't present. The analysis team can also take on responsibilities as a security advisor and develop security strategy based on data captured and analyzed. Members of the analysis team must be analytical and detail-oriented with specific skills in understanding how devices generate logs and how to work with network and security tools that generate logs. Analysis engineers can also be responsible for analyzing and reverse engineering various types of artifacts, requiring a different set of analytical and technical skills than an analyst that works with security logs. Analysis engineers are technical, detail-oriented, and specialized in the types of data they are responsible for analyzing.

Possible job titles include security analyst, security engineer, security administrator, security specialist, security consultant, network engineer, operations analyst, business intelligence analyst, and data analyst.

Compliance Service

The most fundamental skill for employees responsible for compliance is the ability to deal with risk and conflict management. A compliance officer uses specific factors for scoring risk, which will be based on the requirements for the type of compliance being enforced. A compliance officer will encounter situations requiring explaining and defending their point of view to internal employees as well as external agencies such as regulators. Communication and analytical thinking are critical for this role as well as a willingness to learn, as the world of compliance is continuously changing. Other skills associated with successful members of the compliance team are being detailed-oriented, being capable of interpreting data, and having strong problem-solving skills.

Possible job titles include compliance officer, assessment officer, policy officer, and infosec officer.

Digital Forensics Service

Roles in digital forensics are technology-focused, requiring a desire to learn, deep analytical skills, and the ability to work with various technologies ranging from desktop computers to mobile devices. Digital forensics requires acute attention to details and a comprehension of cybersecurity fundamentals.

Communication skills and an understanding of law and criminal investigation are important because the results from a forensic investigation might be used in court, in which case the investigator will be required to defend his or her work. Digital forensics requires working with different groups, from legal to technical, as well as tolerance for disturbing material that might be discovered during an investigation. Successful digital forensic engineers have experience in both legal and technical matters related to cybersecurity.

Possible job titles include forensic engineer, forensic scientist, forensic consultant, and digital forensic engineer.

Situational and Security Awareness Service

The key purpose of this service is to address the human element of security. The goal of the work performed by the situational and security awareness team is to change the behavior of employees so that they operate with security in mind, reducing their risk to the organization. Duties include everything regarding security awareness and developing an education program. Roles responsible for situational and security awareness require strong written and verbal communication skills. Members in this role must be able to interpret all industry regulations, standards, and compliance requirements as well as ensure that everybody understands the organization's risk management strategy. Successful situational and security awareness officers can accomplish these goals using a positive and engaging approach, which includes creating a metrics framework that can effectively measure results of the program.

Possible job titles include security trainer, training instructor, information assurance analyst, training analyst, security service training manager, and development manager.

Research and Development Service

SOC members of the research and development service are responsible for researching, planning, and implementing new programs and protocols for the organization. Duties include market research, tracking costs related to the creation of new programs and protocols, and making decisions on which projects are worth investing in. This group also validates if current programs, procedures, and technology being used are up to date with current and advanced industry standards. Members in this role have project management experience, are able to manage a budget, and are detail-oriented and creative.

Possible job titles include researcher, threat researcher, threat analyst, analyst, security analyst, programmer, software developer, and DevOps engineer.

Soft Skills

Another important element that must be included in your job roles is a description of the required soft skills, or nontechnical capabilities. Soft skills are different from having the technical ability to perform a job role and are just as important as technical skills when considering candidates for your SOC. Let's look deeper into the concept of soft skills.

Soft skills are a combination of people skills, social skills, communication skills, character and personality traits, career attributes, emotional intelligence, and other human-based factors. Identifying the ideal candidate for any job role must include considerations for your position's soft skills along with the expected technical skills (also known as "hard skills") to ensure a successful match is made. For example, if an employee is shy and can't communicate well, he or she would not be ideal for a role that requires that responsibility. I see many companies make the mistake of promoting a person into a manager or team lead role just because that person has many years invested in the company or is a top performer in his or her current position. The soft skills associated with a manager are unique and require leadership attributes, which some employees will not have based on their personalities and social skills. Not considering soft skills when recruiting new people or promoting employees will lead to underperformance in your SOC.

Certain job roles in a SOC require mature soft skills. Any role that involves communication with executives, public relations, or legal parties requires brevity and clarity of communication in both digital and in-person communication. Soft skills must also include adjusting what is being communicated based on the impact it could have on the target audience. SOC roles that interact with executives must also include soft skills that can provide respectful pushback and constructive feedback when necessary.

Certain roles within a SOC are responsible for developing escalation procedures for events and executing those procedures when an event occurs. These types of SOC roles require soft skills for communication to ensure the accuracy of data that is provided as the escalation process occurs. Soft skills also include deciding when to escalate an event, how often the event should be escalated, and how to identify the severity of an incident. Mistakes in communication can cause a breakdown of the escalation process ranging from overlooking severe incidents to wasting resources on non-severe incidents.

Evaluating Soft Skills

What soft skills should you look for as you recruit candidates for your SOC? According to the LinkedIn article "Hiring Without These Critical 'Soft Skills' Is a Recipe for Disaster" by Lou Adler, creator of the Performance-based Hiring methodology, several key hiring mistakes that are not related to technical or soft skills contribute to failure. The first mistake is a mismatch between a manager's style and the new hire's need for management and coaching. Some employees will want guidance and will feel isolated if left alone, while other employees interpret guidance as micromanagement and will not approve of being continuously monitored and managed. It is important for a hiring manager to explain their management style and identify if candidates would be comfortable working in that type of environment. A simple question you could ask candidates to identify their desired management style is, "Are you more comfortable with a hands-on manager or a hands-off manager?" Essentially, you are asking potential new hires if they prefer having periodic interaction or continuous interaction with their direct manager. Experienced managers will be able to adjust their management styles to how their direct reports want to communicate with their manager, the expectations for which can be set upfront during the interview process.

Another soft skill conversation hiring managers should have with potential candidates is about the pace of the organization and expected motivation factors to complete tasks. Organizations work at different speeds, sometimes putting pressure on people to meet specific timelines or encouraging people to work late hours. For example, some organizations may claim to work 9 a.m. to 5 p.m. business hours but frown upon people who leave right at 5 p.m. if work requirements are behind schedule. A hiring manager should be upfront during the interview about how aggressively work schedules are enforced.

People are accustomed to different types of communication styles and expectations. Mismatching communication expectations between a manager and employees can lead to misunderstandings and team underperformance. For example, some people view text messaging as real-time conversation that requires immediate response, while others treat text messages similarly to email, responding to incoming messages when time permits. In this example, somebody with expectations for real-time responses to text messages may interpret not receiving a prompt response as being ignored or as the receiver not wanting to respond, whereas the reality might be that the receiver of the text message believes that text messages should be treated like any other form of communication and prioritized based on importance. Communication style should be confirmed between the hiring manager and candidate, including how often communication should occur and what type of details should be communicated. Examples of reports and data expected to be delivered by employees to their direct manager are great items to go over with a potential candidate to identify if the candidate meets the required soft skills to complete the tasks.

SOC Soft Skills

Specific roles in the SOC have corresponding soft skills expectations, many of which were identified earlier in this chapter as I described skills involving how people communicate and work. I pointed out that some roles have strong organizational and operational skill requirements. Some roles require critical thinking and problem solving. Roles involving interacting with team members require the ability to collaborate with others. Technical writing skills are needed for roles that create reports or develop training. Many of these skills are not developed through technical training but rather are gained through work experience or general education or are just part of a person's personality or natural abilities.

Many SOC managers and directors I speak with are less concerned about a new SOC member's knowledge of specific tools. SOC leaders want a new SOC member to have an understanding of underlying functions, systems, networks, and processes and be able to fit into the SOC culture. Along with a strong work ethic (discussed in the next section), soft skills are a critical evaluation point for many SOC roles. Soft skills tend to be more important than technical skills for many roles.

The following is a list of soft skills that I find are common in members of a SOC regardless of which service they provide. I recommend including these soft skills in job profiles when recruiting.

- **Problem solving:** Industry and market knowledge
- **Analytical skills:** Troubleshooting complex issues
- **Communication:** Business understanding

- **Negotiation and diplomacy:** Work under pressure
- **Detail-oriented:** Organizational skills
- **Teamwork:** Documentation and presentation

Security Clearance Requirements

In addition to the previously discussed hard and soft skill requirements, another factor to consider as you develop a job description is that some roles in the SOC may require certain levels of security clearance in order to have access to specific content. Security clearance can be mandated by the organization and/or by law and is a license issued by an agency, the head of a department, or a branch of the federal government. Many U.S. federal employees and many employees in the private sector are required to obtain security clearance. The amount of time required to obtain any level of security clearance depends on different factors, but according to one source, Security Degree Hub (https://www.securitydegreehub.com), obtaining a U.S.-based security clearance on average takes six months to a year. During a clearance evaluation, various aspects of a candidate are verified, including their identity, where they were born, where they live, who lives with them, any previous or current financial troubles, or anything else that could represent a risk of granting the candidate enough trust for the specific level of clearance they are applying for.

Security clearances have different levels, which grant specific levels of access to classified content. Regarding the U.S. federal government clearance stages, there are three levels, corresponding to the potential impact data loss at that level could have on the government and associated parties:

- **Top Secret:** Highest level of classification. Exposure would cause "exceptionally grave danger."
- **Secret:** Second highest level of classification. Exposure would cause "serious danger."
- **Confidential:** Lowest level of classification. Exposure would cause "damage."

It is important to point out that the U.S. federal government has additional language and classification levels used in classified communities. Some Top Secret clearances indicate the employee has passed a Single Scope Background Investigation (SSBI). This means the employee needs Top Secret clearance and access to sensitive compartmented information (SCI) in order to do their work. This clearance is not the same as an employee granted Top Secret SCI, which represents a SCI program run by a specific agency. SCI programs can ask for additional validation, including polygraph examinations, as part of the screening process, but it is inaccurate to assume that all Top Secret SCI employees have had a polygraph or additional validation beyond what is required for a Top Secret clearance. The requirements for a SCI program are specific to the agency it is assigned to, meaning even if you have Top Secret clearance, you would not be granted access to any material deemed Top Secret SCI unless you have been granted SCI access by the specific agency behind the SCI program. If one SCI program grants an employee Top Secret SCI clearance to its agency's SCI, that does not grant the same employee Top Secret SCI clearance access to any other agency's SCI.

Note

Learn more about the United States Security Clearances program at https://www.state.gov/m/ds/clearances/c10978.htm.

Countries in the European Union (EU) use a similar classification system known as the European Union Classified Information (EUCI) system. The EU approach breaks classified information into four levels. Like the U.S. classification system, each level is based on the potential impact data loss could have on the government and other associated parties.

- **Très Secret UE/EU Top Secret:** The unauthorized disclosure of this information could cause exceptionally grave prejudice to the essential interests of the EU or one or more of the member states.
- **Secret UE/EU Secret:** The unauthorized disclosure of this information could seriously harm the essential interests of the EU or one or more of the member states.
- **Confidentiel UE/EU Confidential:** The unauthorized disclosure of this information could harm the essential interests of the EU or one or more of the member states.
- **Restreint UE/EU Restricted:** The unauthorized disclosure of this information could be disadvantageous to the interests of the EU or one or more of the member states.

Certain groups, such as the General Secretariat of the Council (GSC), provide approval lists for the types of cryptographic products that can be used on certain levels of EUCI classified data. The same policies apply to people, process, and technology associated with EU classified information. Learn more about the EU classification system at https://www.consilium.europa.eu/en/.

The type of clearance your SOC or the organization protected by your SOC will or will not require will be based on the laws governing your organization and the data it is associated with. In some situations, access to content can be granted while a clearance is being processed, known as being in an "interim status" or temporary status. Other times, the clearance process must be completed before access to protected content can be granted. Most security programs require a periodic reinvestigation after a specific length of time, which time will be shorter as the level of clearance is increased. You will need to validate requirements for clearance with somebody that specializes in security clearances, such as a security clearance officer, before you consider providing specialized clearance to any of your employees.

Pre-Interviewing

At this point, I have covered how to create a job role, the different types of roles that exist in the industry, the job roles associated with SOC services, and how both soft skills and technical skills (and perhaps security clearance) should be considered for a job role. You can use all of these factors to develop job requests for the positions that you need to fill as you launch new SOC services or grow existing SOC services. Now it is time to look at how to fill job roles in your SOC with the right people by executing a successful interviewing process.

You will want to create a filtering system to avoid wasting time interviewing unqualified candidates for any job role you are looking to fill. According to a study by ISACA, 57% of respondents note the lack of qualification of half of the candidates they have hired. This feedback translates to half of the candidates seen by ISACA's survey were found to not be able to perform the skills advertised on their resume during the interview process! Qualifying skills is a critical step of the interview process and must be done for any skill required to perform the job you are looking to fill. Candidates will list anything on their resume, from how long they worked in a position to the type of work that they performed; however, it is up to you to validate whether the provided information is true. Make sure to do this early using a prescreening process that includes one or more knockout questions to filter out unqualified candidates.

Candidates can provide proof of their skills through certifications and degrees, which might or might not be current, valid, or completed. Verifying industry-recognized certifications and degrees from accredited universities will be easy and can be done by visiting the provider's website or using a validation service as long as you have the candidate's full name, certification number, and date of graduation if applicable. For example, you can consult the National Student Clearinghouse (https://www.studentclearinghouse.org/) to verify a degree from an accredited school was obtained by a candidate. Verifying certifications and degrees can also be used as part of the knockout process.

Note

A certification does not mean a skillset exists! Certifications show the required skills were validated at a specific point in time. Skillsets must be practiced or they are lost. Many recertification programs do not use the same rigor as the original certification, meaning a recertification date would not reflect the same skills existed as when the original certification was achieved. Some certifications can be cheated through the use of brain dumps, which publish the answers to the exams required to achieve a certification. For all of these reasons, it is important to use your own validation system to verify skills exist rather than depending on an external certification program.

Verifying work experience can be more challenging based on what is provided as a reference point. Things will change over time, including the status of people who worked with the candidate and the status of the organization the candidate worked at, sometimes causing a reference to no longer be available. Some candidates will also ask that you not contact their current employer until an offer is provided, prohibiting any validation of their current skillsets. If you can't speak with the direct manager of a current candidate, ask the candidate if you can contact a coworker or other party that can validate the skills you are looking for in your potential candidate.

Note

It is important to be mindful that some of your strongest candidates will have skills that are represented on the resume in their job experience and not through education or certification programs. I have worked with very capable engineers who do not have a high school degree or certifications. I have also encountered unqualified candidates who have listed dozens of certifications and years of experience on their resume. Make sure to use your own skill assessment process when validating skills.

Avoid using language during any job postings or during a live interview that includes preference for a particular gender, race, age, religion, or other such status. For example, posting "we are looking for a *young* and *energetic* team member" would suggest age discrimination based on the use of "young" and "energetic." You can highlight your organization's view of providing an unbiased recruiting process externally by stating you are an "equal opportunity employer" or stating "nothing in the job posting or description should be construed as an offer or guarantee of employment" in your job posting and during a live interview. Keeping your hiring process unbiased will not only attract a diverse pool of candidates but also help avoid unwanted legal matters in regard to violating people's rights.

Interviewing

Once you have created and posted requirements for your SOC role to be filled, you will need to evaluate the potential candidates. The initial conversation can be a phone call, video conference, or web chat. The focus of the first interview is to exchange information about what is being offered by both the recruiter and the potential candidate to see if a potential match exists. According to Monster, a common mistake made by hiring managers is spending too much time describing or "selling" the position. It is important to also spend time listening to candidates so that you can assess their qualifications, skills, and personal characteristics. Not doing this leads to wasting time with follow-up interviews with candidates that are interested in the opportunity but not qualified or not a good match for the role. It is ideal to include a member of the team that has the job role opening to assist with the interview process, not only to help validate that the candidate's skills are a fit but also to look for potential team chemistry. Candidates' answers regarding specific qualifications or skills should be assessed by experts in those areas to ensure candidates are properly evaluated. Lastly, ensure that any special constraints related to the role are covered upfront, such as required travel or potential overtime.

Interview Prompter

One tool that can be used to standardize the questions delivered during the interview is an interview prompter template specific to the job role. Questions within the prompter can be developed and validated by internal team members and experts in the associated technology prior to the prompter's usage. Experts can also be used later to review the responses that are provided by candidates during the live interviews.

An interview prompter template can include questions about the following:

- General skills
- Specific technical skills
- Educational background
- Years of experience and what the experience involves
- Details about past projects and job roles
- Work the candidate enjoys and doesn't enjoy being involved in
- Career and personal goals
- Limitations and constraints, including salary and overtime availability
- If employed, reason for leaving their current role and considering this role
- Availability to start
- Descriptions about the role
- Overview of the position
- Describe the team
- Company business and culture
- Company benefits
- Compensation system
- Associated projects and expectations

Note

The last seven questions are focused on selling the SOC position while the first questions are designed to learn about the candidate.

The interview prompter template is very helpful for organizing questions, but asking questions in the specific order listed in the prompter isn't required. It is common for an interview to start with the interviewer providing an overview of the opportunity and then letting the conversation flow naturally from topic to topic as questions are asked by either the interviewer or interviewee. The interviewer can check off items on the interview prompter to ensure that all topics are covered within the interview time slot regardless of the order in which the answers are obtained. The prompter also helps ensure that the interviewer covers required topics within the allocated time for the interview using the task checkoff process.

Post Interview

After first-round interviews are conducted, qualified candidates might be asked for a face-to-face follow-up interview. Among the purposes of the second interview are to enable the candidate to meet with the team members or direct manager, to permit the candidate to assess the environment they would be working in if hired, and to have the candidate perform additional skill tests. Skill tests can include hands-on work with tools or applications, logical exams, or other methods to validate the expected knowledge and skills meet what is required to perform the job role. If both parties remain interested after the second interview, the hiring manager should provide a target date for a formal decision regarding whether the candidate will be offered the position. The offer can also occur at the end of the second interview and be verbal if time is required to develop a formal draft of the offer. There may be other circumstances that would postpone a formal offer, such as ensuring the candidate meets substance testing requirements before being formally offered a position.

When developing a formal offer letter, make sure all details are clearly defined. This includes the position, expected tasks, total compensation package, and start date. The offer letter should include the name of the new hire's immediate manager and any additional document(s) that must be brought in on the first day. It is standard practice for the human resources department to develop and provide the offer letter to the new employee rather than the recruiter or hiring manager.

After providing an offer letter, the next stage of the hiring process is onboarding the new employee.

Onboarding Employees

Once a job role is filled, the hiring manager will need to prepare to bring the new employee into the job role. This process is also called *onboarding* the new hire. It is critical to properly prepare for a new employee, both to ensure that the new employee's time isn't wasted waiting beyond the designated day to start work and to ensure that the new employee has a positive first impression of the new job. A new employee will be frustrated if he or she arrives the first day ready to start working but doesn't have a workspace and computer allocated—basic essentials which should be prepared before the new employee arrives. The following list are requirements a hiring manager needs to prepare prior to the new employee's arrival. Provisioning of these items can be done by other team members such as desktop support and human resources, but it is the overall responsibility of the hiring manager to ensure these items are available prior to the arrival of the new employee.

- Allocated physical space within facilities, such as a desk and chair if applicable to the role
- Expected office supplies
- Computing equipment

- Employee identification and credentials such as telephone numbers, user IDs, and passwords
- Special software or tools
- Scheduling of education or overview of job role, if necessary
- Printed or electronic documents on processes, policies, methodologies, and other items relevant to the job role

The hiring manager also needs to prepare other internal team members for the arrival of the new employee. Information such as the background of the new hire should be shared with the direct team. Additional information such as personal interests can be shared to promote a positive chemistry, if disclosure of those details is authorized by the new hire prior to his or her arrival. Skills and duties associated with the job role should be shared and validated with the direct team so expectations for the new hire are clear to everybody.

Onboarding Requirements

Certain SOC roles will have specific onboarding requirements. Those requirements can include obtaining authorization to access sensitive resources, learning existing processes, attending training for new hires, and signing off on required compliance documentation. Some training might involve shadowing employees, with the goal of switching from a monitor to an interactive role as the new hire learns skills and processes. For example, a new hire might be assigned to monitor the incident handling procedure the first month on the job or work on a fake incident before being responsible for interacting with a real incident. Senior team members can review how a fake incident is handled by a new hire and provide coaching and reference to procedures as the new hire transitions into an operational role.

SOCs that follow industry guidelines should have new hires study the guidelines relevant to the job role. An example is having a new hire who is part of the incident response program first review the NIST 800-61 (Rev. 2) *Computer Security Incident Handling Guide* or the FIRST PSIRT Services Framework (introduced in Chapters 1 and 3, respectively). Required reading can also be provided before a new hire starts, which the hiring manager could reference and even quiz the new hire about to ensure learning objectives were achieved the first week they started the new role. Expectations for this material can be shared as part of the expected onboarding process as a new hire’s first few weeks schedule is developed by the hiring manager.

It is critical to ensure a smooth transition into a position for any new hire. The first few weeks will determine if the candidate is a fit for the role and will be capable of handling the associated responsibilities. Part of creating a welcoming environment for employees is properly setting career expectations.

Managing People

Failure to properly manage people will lead to a SOC whose employees are a flight risk, ready to leave for another organization if a better offer comes along. The current IT market is strong, and it will take effort to retain top talent. Great managers know what drives the people who report to them and act as an enabler for those goals. Career-driven people are not focused only on how much money they make. Table 4-13 lists the top five things that make employees happy at work and the top five reasons why employees are not happy and eventually leave a position. This data comes from Monster and BioSpace.

TABLE 4-13 What Makes a Happy or Disgruntled Employee

Happy	Disgruntled
Feel accomplished	Are disengaged
Receive positive reinforcement	Are stressed out
Like their co-workers	Have a negative mindset
Have some level of autonomy	Have poor relationships with managers and colleagues
Are proud of what they are part of	Not fully using their intellect or strengths

As a SOC manager, you will want to identify what motivates each of your SOC employees as well as help guide which future position and goals would be most ideal for them to target. This includes identifying that an employee is working a stepping-stone position with the goal of taking on a more senior role once they acquire the appropriate skills and experience. Goals should be documented in an employee development plan and must benefit both the organization and the employee. Before setting goals for an employee, consider the business goals and how that employee aligns to short-term and longer business objectives. Make sure to consider whether certain roles need to be filled in the future and, if so, whether this employee could be groomed for that needed role. Having a business goal aligned with an employee goal helps justify investment in training and experience so that both parties benefit from the promotion.

Once business goal alignments are identified with potential employee goals, speak with the employee and confirm career aspirations. When a career goal is confirmed by the employee that aligns with the business goal, assess the potential and readiness for the employee to take the role by asking the employee the following questions:

- Would you be able to gain the skills required for the role?
- What skills and experience do you currently have or lack that are required for the role?

Look at the gaps in the readiness assessment and develop a potential timeline to achieve those missing skills and experience. The results of this exercise will provide a development plan that leads to achieving a goal that is good for both the employee and the organization.

Common factors that can act as motivators or discourage an employee from working within a specific job role are as follows:

- Income
- Geographical location

- Travel
- Work/life balance
- Type of work (technical, social, sales driven, etc.)
- Benefits
- Training and experience opportunities

It is important to identify how each of these factors impacts every employee as you create development plans to ensure their personal goals are met along with professional goals. For example, one position might have a higher pay but require more travel, posing an unwanted work-life balance for a particular employee. Another job might pay less but provide the opportunity to live where the employee desires and offer teleworking opportunities, which might be more important than higher pay to a particular employee. Not covering personal goals can lead to moving employees into roles that negatively impact their personal lives, causing the employee to leave regardless of the benefits of the promotion. Consider these personal factors when creating a development plan for your employees.

Job Retention

Often, the term *competitive workplace* refers to competition between existing employees. This view translates to an employee struggling with separating themselves from the other career-driven employees all vying for attention from management to gain a promotion. In the field of cybersecurity, the dynamic has switched in favor of the employee. Now the competition exists at the organizational and corporate levels, leading to organizations shopping for talent within other organizations based on the huge demand for talent. Employees with the right experience and skills will be bombarded with job offers daily, making job retention extremely difficult to maintain across all SOC positions. You need to focus on job retention or all of your time invested in finding the right employees will end up benefiting somebody else that poaches them!

Salary.com suggests a few benefits you can offer to your employees to improve job retention. Offering some of these items might not be possible or cost effective for every employee, but providing them when possible is ideal. The first offering is good health coverage for all employees, including part-time workers. Good healthcare includes wellness benefits such as gym memberships, healthy snacks, and other ways to keep employees healthy and strong along with traditional healthcare services. Healthcare services include preventative benefits, which cover all aspects of physical health, dental care, and vision. Healthcare also includes self-care benefits such as legal services to help with personal matters, discount programs, and mental healthcare. All of this will help reduce personal distractions and keep employees happy.

Salary.com also suggests offering telecommuting opportunities and flexible hours when a job role allows either. These benefits can be offered in small doses, such as once a week or more frequently, depending on whether employees in the role can provide the same value as they provide working in the office on a fixed schedule. Offering telecommuting and flexible hours also increases the geographical reach for recruiting people as well as retaining employees that have to move but still want to be part of the SOC, since they can continue work from their new living location. Factors such as the hours and availability of the SOC as well as location requirements will impact these offerings.

Another benefit suggested by Salary.com is encouraging employee training, workshops, and other forms of education. Offering training opportunities not only develops talent within the organization, but keeps employees motivated to stay and improve their capabilities. Completing training can be used as milestones for raises and other rewards, giving employees a clear direction on how they can advance their career. Make sure to consider all types of training and development, ranging from formal classroom training to on-demand online courses. Other development options outside of training include shadowing senior members for over-the-shoulder training, one-on-one coaching and mentoring, local networking groups, and adding members to special projects outside of their normal job duties. Also consider group rates if a specific skill or certification can be applied to multiple employees to save on training costs.

Some organizations use their investment in training to retain employees by offering to pay for training if the employees commit to remaining in their role or employed by the organization for a specific period of time. The benefit of this approach is that it discourages employees from leaving the organization since they would forfeit having the organization pay for their training. The downside of this approach is possibly discouraging some employees from pursuing training due to their unwillingness to sign a retainer agreement. An alternative to training retainers is to provide compensation awards in the form of stock or pay that pays out over a specific period of time based on the employee remaining within a role or at the organization. This approach also encourages employees who don't want to commit to a retainer to obtain training.

Training

Training is the action of teaching a particular skill or type of behavior. SOC employees need to be trained to be able to perform their jobs and keep up with the changing threat and IT landscape. When an incident occurs, a common corrective action is more training. I already covered how training is used by companies to retain top talent. Considering all of these reasons for investing in training, the costs for training can quickly become a fortune and training results can be hard to measure if specific objectives are not defined. The following are recommended steps and considerations when developing a training program for any SOC employee:

Step 1. **Create the business case:** How does this training impact the SOC and employees that will be attending it? Does the training target a specific SOC service need or is it for career development? A cost-benefit analysis might be needed to justify the requested training.

Step 2. **Define objectives and learning outcome:** Describe what knowledge should be obtained via the training and how to judge if learning objectives were met. This could be achieved in several ways, such as having the employee obtain a certification or demonstrate the new skill.

Step 3. **Select a training method:** There are many methods to deliver training. The traditional in-person class may be more effective than delivering training online, but a live class will cost more both in time and money. Using recordings will reduce the cost of delivering training, but students will not be able to have discussions with the trainer, potentially reducing the quality of the training. Consider all options, including over-the-shoulder training, video, video conferencing, and live classes.

Step 4. **Identify resources:** Who will provide the training? Will it be in-house or an external resource? Are there any qualifications required for somebody to deliver the training properly? Some certification programs require a certified proctor to deliver content, limiting available resources to provide the training.

Step 5. **Develop training material:** Make sure the content that is developed is in line with the training objective identified for the business case of the training. This includes meeting all learning objectives so that candidates who complete the training can be properly qualified as successfully trained.

Step 6. **Deliver training and evaluate effectiveness:** Deliver the training and include a way to obtain feedback. Feedback should come from both the trainer and trainees to best understand both parties' experience of the course.

Step 7. **Improve the training:** The final step is to grade how well trainees accomplished the learning objectives as well as review the feedback from both trainers and trainees. Use these results to adjust the class so that it becomes more effective.

An example of going through this process is considering training for using a specific tool. The business case can be based on the impact the tool will have to a SOC service once the users are properly trained. The outcome of the training could be a certification from the tool vendor as well as the trainee's ability to showcase how they use the tool. The method of training could be a live boot camp delivered by the vendor's training resources or some other method that accomplishes the desired training outcome. The resource and material could be provided by the vendor, but a SOC sponsor can also be involved to help with running the class and obtaining feedback. The cost for this entire process can be computed and weighed against the value of the outcome to properly justify the training before any investments are made.

Training Methods

There are many variations of training, the quality of the results for which will be impacted by the method used. Many cybersecurity concepts require hands-on experience with potentially illegal tools. Certain divisions of the U.S. military such as the U.S. Cyber Command (USCYBERCOM) request contracted training to include working within real-world scenarios that replicate the actual challenges organizations are likely to encounter. Expectations are that the USCYBERCOM candidates will have experience dealing with real malware and defending against genuine exploitation tactics. USCYBERCOM not only requests real-world scenarios but also sets expectations for persistence as part of their success criteria. Persistence means training must be regularly scheduled as well as sometimes unannounced to continually hone skills.

Training might not be project specific. Your SOC employees might want to take on different roles that have certain training requirements to perform properly. Encouraging career growth is key to developing a relationship with employees, leading to employee retention and savings on in-house promotion versus the costs to replace lost employees. Enabling career growth can be accomplished not only through formal training but also using informal over-the-shoulder shadowing of other employees. This approach not only saves in training costs, but also develops redundancy for skillsets and critical personnel. Formal training can also be offered, which can be tied to agreements for a trainee to remain within their role at the organization for a period of time in exchange for the training being paid for by the organization. A violation of the agreement could require the trainee to pay for the training, reducing the likelihood of the employee leaving their role during the agreement period. Promotions and other awards can also be tied to training milestones, which milestones can align with expected skills of more senior job roles defined within your organization. Aligning training and career paths will improve employee retention since employees will have a reason beyond a paycheck to remain in the organization.

Another training consideration is to develop a *cyber range*, the purpose of which is to simulate a real environment and the types of threats that an analyst could encounter. A cyber range might not be tied to a specific learning objective, but can be viewed as a practice ground to help members test out various types of scenarios that will come up as the SOC operates as well as customized scenarios based on specific learning objectives. A cyber range should have a student utilize tools to solve challenges in real time using a similar environment to the SOC's real network. The cyber range should be isolated from the real network, providing a safe, legal environment to gain hands-on skills with tools used by the SOC and expected situations the SOC will encounter. Many guidelines, including the National Initiative for Cybersecurity Education (NICE), define recommendations for a cyber range. One military-based saying that highlights the importance of using a cyber range to gain experience with cyberthreats is "the battlefield is the last place you want to meet your enemy for the first time." It is best to fail in a range rather than in the SOC.

I recommend considerations for training based on real-world scenarios and including criteria for persistence to ensure that employees not only learn skills but retain them. It is not unusual to find that a candidate certified in specific skills isn't able to perform those skills after a prolonged period of time of not using them. This brings us to an important concept, which is understanding the relationship between certifications and training.

Certifications

An IT certification validates that the certified professional has competency in a specific aspect of technology. Each certification program has its own method to validate a candidate's skills, which range from combinations of test takers answering multiple-choice questions to performing hands-on exercises. After a candidate's skills are validated through a program's assessment process, the program issues a certificate signifying the person met the program's requirements and the specific date on which the certificate was issued. Many programs require a recertification assessment within a certain period of time after initial certification. Recertification requirements vary from program to program and can involve either performing the same skills required for the initial certification, using a condensed version of the testing system, or just paying a fee, typically used to fund a membership program. Do not assume that a certification validates a person's *current* skill level; take into consideration when the individual was certified, what was involved to get certified, and how often recertification occurs. The best approach to validate any skill is to have the person perform that skill in your own real-world scenario.

One common challenge I hear from SOC managers is determining which certification is the best option for their employees. My advice is to consider aligning the purpose for a certification program with the SOC position looking to get certified. Certain certifications and training are designed for specific job roles. For example, the CompTIA CySA+ is designed for a cybersecurity analyst, while the EC-Council Certified Penetration Tester is obviously targeting the penetration testing market. I included suggested certifications for each job role related to SOC work earlier in this chapter.

Evaluating Training Providers

Different training providers will offer their own version of a certification program. For example, EC-Council, SANS, and Offensive Security all offer a penetration testing certification. Some of the content will be similar, while other parts of the program will be unique based on how the provider develops its material. It is recommended to consider the following when evaluating a program:

1. What steps/efforts are required to learn and achieve a certification?
2. What are the upfront and annual costs following completing the certification? Some programs require recurring fees.
3. What are the recertification requirements?
4. How respected is the certification/program based on industry feedback?
5. Do the learning objectives align with your own learning objectives?
6. Who will be developing the content and teaching the content? Some programs push live classes with generic teachers that provide little value for the high cost of the course.
7. When is the training offered and does it meet your training timeline?
8. Are there better competitive training options that accomplish similar learning objectives?
9. Does the training and testing format mesh with your learning style?

Training should not be limited to individual learning or technical knowledge. The SOC should also train as a unit to improve its services. One popular approach to accomplish SOC training is performing tabletop exercises.

Company Culture

One key factor that is outside of the power of an employee's manager that will encourage or discourage an employee to stay within a role is the company culture. Company culture is the personality of a company. Company culture is a mix of various ingredients including the work environment, company mission, ethics, and values. Some organizations operate in a very casual manner, while others enforce strict rules and regulations. The Balance Careers (https://www.thebalancecareers.com), a service covering career advice, points out that employees enjoy work when their needs and values are consistent with those in the workplace. This leads to employees developing better relationships with coworkers and being even more productive. The Balance Careers also points out that if you don't fit in with company culture, you are likely to take far less pleasure from your work. Forcing an employee that prefers to work independently to work in a team environment will not yield a happy employee.

I have seen organizations attempt to create, and sometimes force employee participation in, what leadership believes would be considered "fun and desired" exercises, which sometimes works very well but often has the opposite effect. For example, an organization might invest in team-building events rather than training, or offer free lunch rather than more paid time off. Some organizations might attempt to push the concept of work culture by changing the language used about the work being done. An example is labeling a call center a "customer satisfaction center." Some organizations might develop sales or service contests such as having the sales team perform customer sales pitches to team members for a chance to win the best sales pitch award. All of these processes are designed to impact people with hopes of improving the organization's culture. I highly recommend any of these actions as long as they align with a business goal that can be measured. If running a team-building exercise or sales contest, make sure to also establish a goal that can be measured following the event. If free lunch is going to be provided, what is the return on this investment and, more importantly, does this have the impact intended and, if so, is it the best option to obtain that impact? Make sure to use a combination of the business strategy alignment techniques covered earlier in this book along with employee surveys to develop processes and other activities that will lead to a great culture. Don't force events for the sake of culture or you will upset some employees as well as waste time and money on efforts that do not positively impact the organization.

Summary

This chapter opened by highlighting the importance of the people within your SOC. You learned about industry job roles to give you an idea of expected skills based on common job titles. Next, you learned about the different SOC services and focused on the expected skills of the people that provide those services. Another important topic covered was the concept of soft skills and how they should be considered as you recruit employees for your SOC. You also learned about security clearance requirements. All of this data is designed to develop job requirements to fill your SOC with the right people as you launch or mature different SOC services.

The second part of this chapter provided recommendations for developing an interview plan, including using an interview prompter to ensure that all questions are covered during a formal interview. It also covered many topics that need to occur after interviewing, including recommendations for bringing new hires into the organization and management best practices to ensure you retain top talent. The chapter closed with a look at training, certificates, and company culture, which all impact retaining top talent.

Next up is Chapter 5, which reviews all the types of data that will be generated by a SOC and how to centrally manage and benefit from those results.

References

Adler, L. (2019, April 29). Hiring Without These Critical "Soft Skills" Is a Recipe for Disaster. LinkedIn. https://www.linkedin.com/pulse/hiring-without-critical-soft-skills-recipe-disaster-lou-adler/?trk=eml-email_feed_ecosystem_digest_01-recommended_articles-5-Unknown&midToken=AQGIjIs7uSiggQ&fromEmail=fromEmail&ut=2DzrO73wb7TUI1

BDC. (n.d.). How to Hire the Right People for Your Business. BDC. https://www.bdc.ca/en/articles-tools/employees/recruit/pages/7-steps-recruiting-right-people.aspx

Berkowitz, M. (n.d.). Think Before You Hire: Maintain a Legal Hiring Process. Monster. https://hiring.monster.com/hr/hr-best-practices/recruiting-hiring-advice/acquiring-job-candidates/legal-hiring-process.aspx

Cotter, T. (n.d.). Evaluate Candidates with a Pre-employment Assessment Test. Workable. https://resources.workable.com/blog/skills-assessment

GetEducated. (n.d.). 13 Highest Paying Technology Careers. GetEducated. https://www.geteducated.com/careers/highest-paying-technology-careers

Indeed. (n.d.). How to Write a Job Description. Indeed. https://www.indeed.com/hire/how-to-write-a-job-description

Jones, G. (2014, June 16). 8 Key Elements of an Effective training Program: Design, Measurement, Continuous Improvement Important. Canadian Occupational Safety. https://www.thesafetymag.com/ca/news/opinion/8-key-elements-of-an-effective-training-program/187061

Mayhew, R. (n.d.). Legal Requirements of Job Descriptions. Chron. https://work.chron.com/legal-requirements-job-descriptions-20506.html

Monster. (n.d.). How to Write a Job Description. Monster. https://hiring.monster.com/employer-resources/recruiting-strategies/talent-acquisition/writing-job-descriptions/

Monster. (n.d.). Keep the Interview Legal. Monster. https://hiring.monster.com/employer-resources/recruiting-strategies/interviewing-candidates/legal-job-interview-questions/

Oltsik, J. (2018, January 11). Research Suggests Cybersecurity Skills Shortage Is Getting Worse. CSO. https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html

Pingboard. (n.d.). 10 Ways to Encourage a Healthy Work-Life Balance for Employees. Pingboard. https://pingboard.com/work-life-balance/

Security Degree Hub. (n.d.). What Is a Security Clearance? Security Degree Hub. https://www.securitydegreehub.com/what-is-a-security-clearance/

ISACA. (2020, February 24). ISACA's Cybersecurity Study Reveals Struggles with Hiring and Retention Persist, More Diversity Progress Needed. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isacas-cybersecurity-study-reveals-struggles-with-hiring-and-retention-persist-more

Index