SOC ANALYST NOW!

TYLER WALL

CONTENTS

Introduction ---- 4
- Cybersecurity: Hot, Hot, Hot ---- 4
- Bumps and Bruises ---- 5
- The Infosec Advantage ---- 5

The Demand for Cybersecurity ---- 7
- Cybersecurity During a Crisis ---- 8
- Demand for Cybersecurity Analysts ---- 9
- Demand for SOC Analysts ---- 11
- What This Book is About ---- 12
- Don't Stop Believin' ---- 14
- Chapter 1 Quiz ---- 15

Areas of Expertise in Cybersecurity ---- 17
- Information Security ---- 18
- Internal Teams ---- 21
- External Teams ---- 24
- Chapter 2 Quiz ---- 28

Job Hunting ---- 30
- Networking ---- 31
- Applying for Jobs ---- 33
- Job Sites and Job Titles for the Win ---- 34
- Common Interview Questions ---- 35
- Tips for a Killer Interview ---- 36
- Chapter 3 Quiz ---- 38

Prerequisite Skills ---- 40
- Networking ---- 41
- Network Security ---- 45
- Cryptography ---- 45
- Endpoint Security ---- 46
- Chapter 4 Quiz ---- 49

The SOC Analyst ---- 51
- Tools of the Trade ---- 52
- Definitions ---- 55
- Chapter 5 Quiz ---- 57

SOC in the Clouds ---- 59
What is Cloud Computing? ---- 60
Fast Facts ---- 60
Cloud Service Models ---- 61
Cloud Security ---- 62
Chapter 6 Quiz ---- 63
SOC Automation ---- 65
What is SOC Automation? ---- 66
Why Automate? ---- 67
SOC Maturity ---- 68
How to Start Automating ---- 69
Sample Use Cases ---- 71
Chapter 7 Quiz ---- 72
Quiz Answers ---- 74
Chapter 1 Quiz Answers ---- 74
Chapter 2 Quiz Answers ---- 76
Chapter 3 Quiz Answers ---- 78
Chapter 4 Quiz Answers ---- 80
Chapter 5 Quiz Answers ---- 82
Chapter 6 Quiz Answers ---- 84
Chapter 7 Quiz Answers ---- 86

INTRODUCTION

Hello there! Welcome to the course that will jump-start your SOC Analyst career and transform your future!

I'm so glad you're here, and I want to assure you that you've come to the right place!

Whether you're arriving fresh out of college or making a career change, I applaud you.

I know it's not always easy to enter a new career field, so I admire you for seeking out your dreams and making them come true, whatever the obstacles.

As such, let's not waste any time!

We'll dive right into the world of cybersecurity, get in on the action, and capitalize on your knowledge for a fulfilling career and satisfying salary.

Cybersecurity: Hot, Hot, Hot

As you probably already know, cybersecurity is a sizzling hot field.

I mean, the cup for cybersecurity jobs literally runneth over.

In fact, as of May 2021, there were nearly 500,000 open jobs in cybersecurity in the United States alone, according to CBS News.

Whoa. That's enough to employ half the population of Austin, Texas or Jacksonville, Florida! Nearly unfathomable.

So it's fair to say that opportunity abounds in cybersecurity!

Let me share an insider secret that you'll be happy to know, though.

While you'll discover nearly endless cybersecurity job listings, the candidates applying for those positions don't always have the right stuff.

In other words, those applicants may not have the skills needed to fill that position.

Or the ones who do have the skills instead elect to enter artificial intelligence, software development, data science, or robotics.

This bodes well for you, though!

That ideal position you have your eye on when scrolling through open jobs? Or that company you'd love to work for, if you only had an inside connection?

We'll give you a leg up on those.

Through this course, you'll gain the up-close and personal access needed for insider tips and tricks to begin a thriving SOC analyst career. You're well on your way to being the SOC analyst candidate with the "right stuff!"

Bumps and Bruises

Now, I'll admit that the road to cybersecurity success is usually a bit windy--and even a little unpredictable.

Accordingly, few candidates go from Point A to Point B and find success overnight.

As with all things worth achieving, you'll need to put in a fair amount of effort and determination.

You might be wondering what that means for you?

We're just asking that you mentally prepare yourself for the trek ahead and stick with us through the course.

In other words, don't give up before the finish line when success is within reach!

Now, I trust that you have at least baseline technical skills to qualify for your dream job. I might not be much help if you don't.

Additionally, a significant portion of working in cybersecurity comes down to getting your foot in the door.

But this...this we can help you with!

The Infosec Advantage

Before we dive into Chapter 1, let me share about infosec, an incredible resource for experienced and inexperienced technology lovers alike. The cybersecurity world offers all kinds of communities to accommodate just about every individual and every interest. Their goal is to provide a sense of community for those in the cybersecurity space.

And honestly, you simply won't find that kind of support outside of infosec.

Trust me. There are so many incredible people waiting to connect with you on infosec based on similar interests or backgrounds. Things that perhaps your spouse or significant other just don't understand because they aren't in the cybersecurity world.

So dig into the various communities offered by infosec--there are a lot--and find your space and your people.

This asset alone will further propel you toward your dream career!

Now we're ready to hit Chapter 1. First, though, my initial recommendation might really surprise you.

Ergonomics is important. You're gonna need an exceptional office chair.

Find one, and then let's get this party started.

THE DEMAND FOR CYBERSECURITY



I probably don't have to remind you what 2020 dropped in our laps...good ol' COVID-19 by way of an unprecedented global pandemic.

As a result, a significant portion of our world shut down.

Entire countries were ordered to shelter in place.

Travel was forbidden. Borders were closed. Trade restrictions were implemented.

Many of us lost jobs. Small businesses closed permanently.

And most devastating of all, some of us lost loved ones. Sorrowfully, we were denied the chance to visit them or honor their lives with a proper memorial service.

I think it's safe to say that COVID rocked our world permanently and is an ongoing worldwide crisis that won't be soon forgotten. It changed cybersecurity, too.

Let's look at how.

Cybersecurity During a Crisis

When it comes to cybersecurity and COVID, it was an interesting combination.

One result of the pandemic was that many jobs continued by transitioning to a work-from-home structure.

This required internet service providers (ISPs) to step up their game, handle spikes in traffic, and ensure the increased demand for video-conferencing was properly met.

But it also allowed some of us to work in our comfy sweats without leaving the house for days, so it was a bit of a win-win in that aspect.

Additionally, The United States Department of Homeland Security designated cybersecurity personnel as essential workers (boy, did we ever become familiar with that term) for continued infrastructure viability. As a result, the demand for cybersecurity personnel soared to a high not previously experienced.

This shortage of qualified cybersecurity workers paired with the pandemic created a perfect storm. After all, an emergency situation like COVID doesn't allow time to train up the needed workers.

As a result, the current cybersecurity workforce had to take on demanding, nearly-impossible hours, and unfortunately, compromise their own physical and mental well-being in the process

But without enough people to fill cybersecurity jobs, there wasn't another solution. The need for cybersecurity help, already in high demand for qualified workers, expanded exponentially overnight.

Here's where the perfect storm occurs: there were no fast fixes.

We did learn a few lessons from COVID, though. It proved an extensive workforce could work productively from home, something we expect will be a normal way of working in the future.

With this situation in mind, let's turn our attention to the demand for cybersecurity analysts and how this career field needs individuals like you who are interested in fighting cybercrime.

Demand for Cybersecurity Analysts

Thanks to cybercriminals, every industry in every country is being targeted. Really, I can't think of even one business that's truly immune from hacker attempts.

And kind of like Arnold Schwarzenegger in the 1984 blockbuster movie, The Terminator, no matter what kind of defense is implemented to block those cybercriminals, *they'll be back.*

Just ask Sony Pictures, who lost a reported $75 million after a data breach, or Capital One, who had 100 million consumer credit applications stolen in 2019. In those applications, over 140,000 US Social Security Numbers were leaked.

Ouch. Yes, cybercriminals are becoming exceedingly creative, crafty, and innovative in finding new ways to penetrate networks.

You just can't keep these guys down.

And it's taken companies some time to realize their vulnerability. It's really only been in the last five years or so that businesses started realizing the need for a solid cybersecurity force.

And the need is big.

Huge.

Colossal.

Accordingly, The US Bureau of Labor Statistics projects that the cybersecurity analyst field is projected to grow 32% by the year 2028. We can compare this to the anticipated growth projected for other computer-related fields, just 12%, and total growth projected for all occupations, just 5%.

Let that sink in: a 32% growth for cybersecurity careers by 2028.

Pretty impressive numbers, right? And a fantastic time for you to take this course, expand your skill set, and get in on the action.

In this course, we'll cover the different entry points to cybersecurity analyst positions, so stay tuned, but I will say that college is not the only path to a lucrative career in the field.

Now that we've established the need in cybersecurity, let's look at how companies are beginning to implement cybersecurity measures.

As the demand increases and organizations begin to embrace the need for cybersecurity, they typically start by forming a Security Operations Center, or SOC.

An SOC has authority over triage, investigation, and response to cybersecurity incidents. This isn't a new concept--law enforcement agencies and the military have used Tactical Operations Centers, or TOC, for decades to manage conflicts.

So like the TOC, the SOC acts as the Command and Control (C2) hub to handle cybersecurity incidents.

A cybersecurity incident is properly defined as an adverse network event in an information system or network or the threat of the occurrence of such an event.

So while the SOC is tasked with responding to cybersecurity incidents, other teams may exist to help in the effort. For example, a Digital Forensics and Incident Response (DFIR) team offers support to the SOC in investigations and response. In fact, the DFIR often takes over long-term investigations, allowing the SOC to focus on daily operations and live incidents.

DFIR team members often have similar skills to SOC analysts, but they usually have a more intense focus on the legal requirements of digital forensics and evidence collection.

Additionally, most of them started out as SOC analysts.

So let's get to the good stuff--the reason you're taking this course.

Demand for SOC Analysts

The entire goal of this course is to prepare you for a career as an SOC analyst, but first let's acknowledge the challenges.

Whether you're a military member transitioning to the civilian world, a recent college graduate, or someone already working in IT, becoming an SOC analyst is an excellent entry point to get your start in the industry. And we're here to help make that happen.

There are a few insider tips you'll want to know.

Though all hiring managers in all industries face challenges, let's look at three that are unique to hiring managers when staffing an SOC.

First, in an SOC, a revolving door of staff presents a unique challenge. Let's say a company hires a new analyst, spends months training them, and then loses them to headhunters from another company, usually offering more money. Frustrating, right?!

It happens frequently. In fact, the average lifetime of a security analyst is just 1-3 years with a single company, so the industry has responded by trying to retain talent. Many companies offer lucrative compensation packages based on how long an employee has been with their organization. A common practice is to spread out stock options over 3-4 years so the worker stays.

Next, another challenge for hiring managers is that SOC analyst burnout is real. The work can be exhausting. SOC analysts often work long shifts with 8, 10, and even 12-hour days.

In addition, they may work overnight shifts. With such fatigue, it's easy to get complacent with monotonous work. It's well known that workers in SOC often have brilliant minds that require challenges.

Lastly, hiring managers have to contend with an SOC being a 24/7/365 operation. Just like the bandits in Home Alone who target rich neighborhoods at Christmas, cybercriminals also don't take a break.

As such, an SOC must be properly manned. International companies have taken a unique approach to this, using a "follow the sun" model--which requires building three SOCs in varying geographical locations to ensure 24-hour coverage. For instance, a first SOC may be in the US, a second in Singapore or Australia, and a third in India or Europe.

Often, though, companies may need an analyst from a specific nationality to work with their data; this is especially true when staffing a Managed Security Services Provider (MSSP).

Back to hiring managers dealing with the 24/7 grind, it can be difficult to find SOC analysts who are willing to work early mornings, overnights, weekends, or holidays. People just don't want to work those hours, or if they do, they soon want to move to regular business hours. It's nobody's fault, but this is an ongoing challenge of SOC work.

Keep in mind that, if you're asked to work shifts like this, you may want to frame it as a temporary sacrifice to gain valuable experience in the industry.

Let's give Tyler the mic to share his experience:

> My first security job was working as a second-shift analyst in an SOC at an MSSP. I was at a place in life where I could handle the demand. Who needed to get up before noon, anyway? I had a base salary and a small shift differential on top of that for working the second shift. It was a year of sacrifice on my part, but it was well worth it. While I eventually longed for the day shift to open up, I knew I was gaining invaluable experience that would serve me well in my future career--and it's still benefiting me and my career today.

I think Tyler has made a relevant point. And since there are many SOC analyst positions that need filled and the demand isn't going away anytime soon, these short-term challenges can present opportunities for you.

With that in mind, the SOC analyst demand continues to grow with every new privacy law and every new compliance and regulation that companies must follow.

In summary, friend, there's no time like the present to pursue an SOC analyst career. If nothing else, this section confirms that qualified cybersecurity professionals are in short supply, opening a door to your next career.

What This Book is About

Beyond the challenges of the pandemic and a shortage of workers, the internet has essentially become a global war zone, providing another critical reason cybersecurity is in high demand.

The constant threat of hackers means our industry desperately needs qualified and trained cybersecurity workers. Proficient employees are necessary to protect companies from continuing attacks and respond effectively when an attacker gets through the barricades.

With such a high need, nearly endless opportunities exist for qualified professionals.

By qualified, we mean the following:

- You are technically skilled.
- You speak the cyber language and possess an understanding of common terms.
- You understand the general structure and expectations while in a SOC.
- You have familiarity with common tools and techniques.

Don't worry if you don't have all of this down just yet. We'll get there in this course.

Before we move forward, let's briefly compare MSSPs and SOCs for your understanding.

- **Managed Security Services Providers** (MSSPs) sell security solutions to customers, and many of their roles are customer-facing. MSSPs tend to have a more robust hierarchy and sometimes include a position like an SOC director. Security is how MSSPs make money, so their culture is centered around that. Additionally, the CEO is always the security guy.

- **Security Operation Centers** (SOCs) tend to have more control over the company's security architecture and engineering. Their analysts go deeply into the infrastructure and learn the ins and outs of the network. Their customer is the company itself. SOC analysts are given more power to intervene during security incidents to remediate the situation. Unfortunately, one bad decision can negatively impact an entire network and become a "resume-generating event," or when an analyst needs to find another job--and not in a good way!

As you venture farther into cybersecurity, this type of knowledge will become second nature to you, like breathing. Before you reach that comfort level, though, there may be some areas that make you feel like a duck out of water.

No worries. We've got you

Don’t Stop Believin’

Beginning a job in an SOC can feel overwhelming. You might not know all the buzzwords. Perhaps there are security tools you don’t know. There could be technologies not covered in your formal education. And if you’re considered an expert in your field, people may inundate you for direction and advice.

With this in mind, you may need a year to get settled. And that’s okay. Give yourself some grace and be patient. Our goal is to help lessen your discomfort in the early days. We’ll help you by familiarizing you with the tools you might encounter on a daily basis.

So with three million current cybersecurity professionals and twice that needed to meet the increasing demand, your skills and qualifications should help you land a job. While plenty of people want the salaries and lifestyles of the industry’s best, you’ll stand out from the crowd by being the right kind of applicant.

Just muster up all your strength, and don’t stop believing in your next career stop.

Chapter 1 Quiz

1. Which of the following companies had 100 million consumer credit applications stolen in 2019?

a. American Express
b. Citibank
c. Chase
d. Capital One

2. SOC stands for _____.

a. Standard Operations Committee
b. Security Operations Center
c. Security Operations Committee
d. Security Oasis Center

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

a. incident
b. matter
c. mistake
d. casualty

4. All the following are true about Digital Forensics and Incident Response teams except:

a. They offer support to the SOC
b. They often take over long-term investigations
c. They often have similar skills to SOC analysts
d. They aren't focused on legal requirements for digital forensics

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

a. Having more qualified SOC applicants than open positions
b. Training a new SOC analyst and then losing them to another company
c. Dealing with analyst burnout
d. Staffing a 24/7/365 operation

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

a. Chase the moon
b. Follow the sun
c. Ignore the clock
d. Avoid UV rays

7. MSSP stands for _____.

a. Management Super Secure Provider
b. Managed Security Shield Producer
c. Management Safeguarded Shield Provider
d. Managed Security Services Provider

8. All the following are true about MSSPs except:

a. They sell security solutions
b. They go deeply into the infrastructure to learn the ins and outs of a network
c. They have a more robust hierarchy
d. The CEO is the security guy

9. The authors of this course say it could take _____ to settle into a new SOC analyst role.

a. 60 days
b. Three months
c. Six months
d. one year

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

a. Emotional
b. Creative
c. Analytical
d. Abstract

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

a. highest
b. lowest
c. longest
d. maximum

AREAS OF EXPERTISE IN CYBERSECURITY



Welcome back! We're entering Chapter 2, which focuses on the many disciplines that make up a successful company, their scope of duties, and how those roles come in contact with the SOC.

Additionally, we'll consider the external organizations that the SOC might interact with on a day-to-day basis.

Because a security investigation could involve everyone in an organization, including the CEO, you'll want to understand an SOC's role in the functions of other teams. In particular, we'll consider three sections: information security teams, internal teams, and external teams.

We'll start our probe by looking at information security teams.

Information Security

Organizations are made up of different teams. Just like a Human Resources department might have focused staff for Recruitment, Employee Benefits, and Training and Development, security teams are broken down into specific areas, too.

Accordingly, information security teams, at least in larger organizations, typically consist of three groups:



Just like everything in smaller organizations, though, it's possible that one or more of these teams may be combined in an effort to save costs. For example, in small organizations, a handful of cybersecurity professionals might handle all areas mentioned above--and more!

So the size of a company's network usually determines if these responsibilities are handled in-house or outsourced to a third party organization.

Let's look closely at different areas of expertise in cybersecurity for a "big picture" understanding:

AREA OF EXPERTISE	PURPOSE	DETAILS TO KNOW
SECURITY OPERATIONS CENTER (SOC)	• Monitors, investigates, and remediates security events	• If internal, the SOC has higher privileges and more extensive knowledge of the network • If externally sourced to an MSSP, then the incident is reported to the IT team. MSSPs often monitor several
THREAT INTELLIGENCE (TI)	• Researches new threats • Determines if threats are dangerous • Provides details to management and other IT teams	• Usually a smaller team. • Sometimes manages the Threat Intelligence Platform, the single point of collection for indicators of compromise and intelligence reports from multiple intel sources. • Typical intel sources of threat feeds include AlienVault or Talos Intelligence and Open Source Intelligence (OSINT). ◦ Commercial threat feeds require a subscription and may be expensive.
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR)	• Takes over incidents from the SOC • Conducts investigations on long and enduring incidents • Often works hand-in-hand with teams outside of the SOC and communicates with executive management concerning high priority cybersecurity incidents	• Acts as subject matter experts • Investigates incidents pertaining to legal, privacy, fraud, or external law enforcement organizations

AREA OF EXPERTISE	PURPOSE	DETAILS TO KNOW
SECURITY ARCHITECTURE	• Focuses on enforcing the best security practices and compliance controls • Implements new technology	• Usually present in larger organizations • -Typically made up of senior security specialists with several years of experience in cybersecurity • -Sometimes outsourced due to limited scope • -Commonly has specialists with specific skills. For example: ◦ Host-based security ◦ Network security ◦ Virtualization or cloud security • -Represents the typical path for SOC analysts to move up after 7-10 years of cybersecurity experience
SECURITY ENGINEERING	• Deploys, manages, and maintains security tools and appliances • Updates and tunes cybersecurity tools • Serves SOC as their number one customer	• Sometimes combined with SOC analyst positions in small companies • -Large companies typically staff internally • -One technology area will usually be assigned per engineer • -Another area for SOC analysts to advance
VULNERABILITY MANAGEMENT	• Identifies, catalogs, and remediates new and existing vulnerabilities throughout the network • -Performs cyclic penetration tests, known as “Red Teams”	• Sometimes outsourced to a consulting company • -Uses vulnerability scanners like Nessus, OpenVAS, and BurpSuite • -Penetration testing may be outsourced

To neatly summarize the information in this table, you just need to know that most organizations have some combination of these roles and teams. And whether the SOC outsources or owns these responsibilities, every company has these functions.

In fact, you can think of each component as a puzzle piece that comes together to create a well-rounded, rockstar cybersecurity program.

Regardless of what team you work on, remember that they're all important to each other. After all, when a piece is missing, the puzzle isn't complete.

And what technology geek doesn't love a good puzzle?!

With information security behind us, we'll now dive into internal teams and how you'll interact with them as an SOC analyst.

Internal Teams

We've covered the roles you'll interact with as an SOC analyst, and you have a foundational understanding of the teams and a general sense of how they operate.

It's time to uncover and define the roles within an internal team. Here we go!

Like every organization, someone's in charge. Whether that person is the CEO, director, or manager, you'll report to a supervisor.

And this person is often powerful. The buck often stops with them when it comes to making business decisions. Let's look at what that might be for an SOC analyst.

We'll start from the bottom and make our way up the chain.

1. SOC Manager: The SOC manager is the first level of management and represents one of the most difficult jobs in cybersecurity. Generally, the SOC manager:

- Handles your offer letter in the beginning
- Approves your compensation, bonuses, and promotions
- Oversees tim e-off requests, work schedules, and your specific SOC duties
- Generates reports to upper management on the number and type of security events
- Ensures upper management is informed on the latest trends of cybersecurity attacks

While this is a brief introduction, we'll cover the SOC Manager in more detail later in the course.

2. **SOC Director:** This title differs across organizations, but you might hear any of the following:

    - Director of Security Operations
    - Director of Threat Management
    - Director of IT Security

    No matter what you call them, this position supervises the SOC Manager. Their general responsibilities include:

    - Handling the overall strategic decision for cybersecurity, including budgets and staffing approval
    - Reporting to Executive Leadership
    - Coordinating with other directors to plan joint projects

    With these facts in mind, we'll also discuss the SOC Director more later in the course.

3. **Chief Information Security Officer or CISO:** The CISO may have a wide range of responsibilities across different companies, but suffice it to say that they're responsible for high-level decisions regarding information security. The CISO is likely the first executive you'll meet and they often will report to the CEO or CTO. It goes without saying that an excellent first impression with the CISO will be an investment in your future career!

With the management ladder loosely defined, now let's look at the internal teams you will work with as an SOC analyst: risk management, governance and compliance, and privacy and legal.

1. **Risk Management Team** responsibilities include:

    - Measuring, reporting, and mitigating an organization's risk levels
    - Considering the likelihood of a compromise
    - Determining the impact if a compromise occurs
    - Generating a report to management on the risk

    Risk Management focuses on the worst-case scenario. Keep in mind, however, they may not be cybersecurity experts. Their understanding of attacks and compromises may be pretty limited, but they do seek to uncover the dangerous outcomes for an organization and how often that may occur.

2. Governance and Compliance Team responsibilities include:

- Ensuring the overall management approach that board members and senior executives use to control and direct an organization is correct
- Communicating compliance standards to the staff and making sure they meet industry standards
- Understanding global compliance standards and their varying sets of controls
- Securing that proper cybersecurity practices are followed in a uniform manner

With this in mind, some of the most common compliance standards are included here for your reference.

COMPLIANCE STANDARD	WEBSITE
Payment Card Industry Data Security Standard (PCI DSS)	*https://www.pcisecuritystands.org*
International Organization for Standardization (ISO 27001)	*https://www.iso.org/*
Cybersecutiry Maturity Model Certification (CMMC)	*https://www.acq.osd.mil/cmmc/*
health insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule	*https://www.hhs.gov/hippa/for.professionals/security/*
Information Security Registered Assessors Progam (IRAP)	*https://www.cyber.gov.au/irap/*
System and Organization Controls (SOC)	*https://www.aicpa.org/interestareas/frc/*

Can you imagine the regulations that must be followed in all of these areas of compliance?! Thankfully, you won't have to. Governance and Compliance is on the job of ensuring everything is on the up and up so you can focus on your job on the SOC.

As an SOC team member, you may interact with Governance and Compliance during audits because the SOC plays a crucial role in providing compliance evidence. Governance and Compliance may request logs, documentation, and security event walk-throughs from the SOC.

3. Privacy and Legal Team responsibilities include:

- Collecting evidence of a compromise
- Identifying the nature of stolen data
- Informing executive leadership on disclosure requirements, legal obligations, and options for pursuing attackers

Remember the Capital One breach we discussed earlier in the course? A Privacy and Legal team would handle the above responsibilities in a

situation like that. As an SOC analyst, you'd likely interact with Privacy and Legal after some type of serious cybersecurity incident and help provide necessary information.

Whew! There were several Internal Team roles to meet. With an understanding of what goes on inside an organization with an SOC, let's now turn to external teams that you may interact with as a future SOC analyst.

External Teams

For our purposes, any team that doesn't work within your company is an external team. We've talked about how you'll interact with information security and internal teams, but communicating with external teams requires different considerations. Let's look at the potential players on external teams.

1. **Government agencie**s are essential in any country, and it's no different for the good old U S of A. SOCs will find themselves interacting with local or federal governments at some point, whether it's for data breaches, compliance, or privacy law interpretation. We strongly urge you to research laws and regulations in your region so that you know what to expect when interacting with government agencies. Let's look at three specific kinds you'll likely come in contact with:

    - Law enforcement agencies represent the most common interactions you'll have as an SOC analyst, and those will typically include issues like providing evidence of data breaches or insider threats to an investigating agency. These include the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and state and local police. When communicating with agencies like this, remember the following:

        - State the facts
        - Remain professional
        - Show respect
        - Use common terms since they may not be cybersecurity professionals

    - Military and intelligence agencies make up the next government entities you may interact with. Since the government buys goods and services from many companies

compliance controls and mandatory reporting requirements come into play. Working with the government ensures shared threat intelligence, and companies can do so by accessing the Defense Industrial Base Cybersecurity (DIB CS) program. DIB CS enables companies to share reports, indicators of compromise, and malware samples, all in one central location. The threat reports and alerts are sometimes based on intelligence collected by military or intelligence agenc ies.

- Regulatory agencies are government and non-government bodies created by legislature to set a baseline of standards for a particular field of activity in the private sector. The agency's job is to enforce these standards, and they're usually separated by business sectors. For example, the US Department of Health and Human Services regulates HIPAA compliance standards. Regulatory agencies often ask SOC analysts for evidence to prove compliance with regulations.

2. Auditors play a significant role in regulatory compliance and often cause headaches for the SOC and its employees. Their job includes:

- Understanding compliance standards and which security controls must be taken to satisfy those requirements
- Applying their knowledge and expertise
- Comparing a company's security against compliance standards

Depending on the compliance standards, audits could happen anywhere from 3 months to annually. Let's break down an example of how an auditor might interact with an SOC analyst during a compliance engagement:

EXCERPT FROM PCI CSS QUICK GUIDE

GOALS	PCI DSS REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	3. Protect stored cardholder data.
	4. Encrypt transmission of cardholder data across open, public networks.

EXCERPT FROM PCI CSS QUICK GUIDE

GOALS	PCI DSS REQUIREMENTS
Maintain a vulnerability management program	5. Use and regularly update antivirus software or programs.
	6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know.
	8. Assign a unique ID to each person with computer access.
	9. Restrict physical access to cardholder data
Regularly monitor and test networks ***This is an example of data an SOC may be asked to provide. The SOC would be the team monitoring access to network resources, and an auditor will likely ask to see the SOC's SIEM. Or some will request a live demo or screenshots of the monitoring platform.***	10. Track and monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors.

It's vital to note that an SOC analyst won't likely interact with an auditor directly. Senior analysts or your manager will often handle the contact, and your task may begin with evidence collection.

3. **Vendors** are external product or service providers that have sold your company a product or service. In other words, anything the SOC uses that wasn't created by your company came from a vendor. A vendor might ask you to join a tool demo or proof of concept (POC) evaluation of a security tool. Vendors provide great networking opportunities, providing potential future job opportunities if you ever move away from the SOC.

Ethically, there are some rules when dealing with vendors. Remember--you represent your company. You can ask for new features, but you want to be sure the company won't be billed before an agreement is made. You also want to avoid promising anything to a vendor.

When asked, you should provide honest feedback, including constructive criticism, because vendors take this input back to their company for changes. Do be sure to avoid insensitive comments like "we could build this ourselves" or "this adds zero value"--that is, unless you want to be excluded from future vendor conversations.

Chapter 2 Quiz

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

a. IAM
b. Operations
c. Engineering
d. Architecture

2. The Threat Intelligence team does which of the following?

a. Takes over incidents from the SOC and conducts investigations on long and enduring incidents
b. Researches new threats to enhance detection, determines if they're dangerous, provides details to management and the SOC
c. Focuses on enforcing the best security practices and compliance controls while implementing new technology
d. Deploys, manages, and maintains security tools

3. Relating to responsibilities, the Digital Forensics and Incident Response Team does which of the following?

a. Focuses on enforcing the best security practices and compliance controls while implementing new technology
b. Deploys, manages, and maintains security tools
c. Researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC.
d. Takes over incidents from the SOC and conducts investigations on long and enduring incidents

4. Responsibilities of the Security Architecture team include which of the following?

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

5. The Security Engineering Team covers which of the following tasks?

a. Identifies, catalogs, and remediates new and existing vulnerabilities

b. Takes over incidents from the SOC and conducts investigations on long and enduring incidents
c. Deploys, manages, and maintains security tools
d. Researches new threats, determines if they're dangerous, and provides details to management

6. The Vulnerability Management team is responsible for which of the following?

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

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

a. SOC Director
b. SOC Manager
c. Chief Information Security Officer
d. Risk Management team

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

a. Director of Security Operations
b. Director of Threat Management
c. Director of IT Security
d. Director of Risk Management

9. Which of the following internal teams focuses on the worst-case scenario?

a. Risk Management
b. Governance and Compliance
c. Privacy and Legal
d. Digital Forensics and Incident Response

10. Pertaining to government agencies, the team you'll most likely come in contact with as an SOC analyst is _____.

a. Regulatory agencies
b. Law enforcement
c. Military
d. Intelligence

JOB HUNTING



Welcome to Chapter 3! So far in this course, we've taken an in-depth look at the demand for cybersecurity and the areas of expertise so that you have a foundational understanding of the field. In this chapter, we'll build on these concepts by moving on to job hunting.

Job searching can sometimes be an overwhelming process that can also feel a bit paralyzing.

To save you time and ease the stress of looking for a new position, Chapter 3 will cover the basics of networking, the job search process, applicable job titles, resume tips, common interview questions, and interview recommendations.

As promised, we're taking you on the inside track to SOC analyst success, and that includes the job search.

Networking

Word of mouth. It's a thing! A big thing, actually.

Consider this. Maybe your favorite doctor came from a friend's recommendation. Or perhaps you bought a car based on what your trusted circle said (or the latest issue of Car & Driver magazine) about that make and model. You could've even vacationed at a particular place because your cousin couldn't stop raving about it.

You see, word of mouth can have a huge influence on people.

In marketing, it's used to encourage customers to spread the good news about a brand. So let's say an organization makes a great product or provides a fantastic service. Satisfied customers will gladly tell others about it.

It's free marketing, and it pays big dividends.

With such powerful influence, word of mouth could also lead you to the perfect job. So let's put it to work for you.

Think about it. You probably know a lot of people. It's time to tap into that wealth of knowledge and discuss your career plans with others, particularly your professional connections, who can keep you up to date on the latest trends in cybersecurity.

Beyond using word of mouth to your advantage, we have a few more recommendations, too.

1. 2600.org. For an online organization of support, check out 2600.org. They have deep roots in hacker culture and offer a website, meetup space, conference, and magazine. Their name has a most fascinating story:

> In the 1970s, Captain Crunch cereal offered plastic whistles in their boxes, and that whistle blew at 2600 Hz. How does that relate to hacking? Well, when a hacker blew it into a payphone (okay, it was 50 years ago), the sound allowed them to make free calls because the whistle copied the exact tone needed to make those calls.

This fun bit of trivia, along with many others, and relevant IT news can be found at 2600.

2. Def Con. Def Con is spelled with two words. You need this conference in your life! Though Def Con sounds like an 80s hair band, it's almost a rite of passage for anyone in infosec. Def Con is held each summer in Las Vegas and offers all the bells and whistles for an IT professional. There's so much to do that you won't know where to start! You simply must prioritize attending if you can make it happen.

> Recruiters also show up to Def Con! In fact, we know many people who have been offered jobs on the spot at the conference. You can also volunteer at Def Con to meet people or join a Def Con group if there's one in your area. These groups meet monthly, allowing you to network with your local infosec peers and keep up with what's going on in your industry. And back to the power of word of mouth, we hope you'll pick up a job lead along the way!

3. BSides. This is another conference held in many large cities, and it also usually meets alongside Def Con in Las Vegas. BSides is growing in popularity and offers a lot of value. You can get inexpensive tickets, and like Def Con, you can volunteer in order to get up close and personal with the events and people.

4. Open Web Application Security Project (OWASP). This nonprofit foundation strives to improve the security of software. OWASP impressively touts community-led open-source software projects, hundreds of local chapters worldwide, and tens of thousands of members. Their conferences take the lead in education and training, serving as a source for developers and technologists to secure the Web--and meet like-minded people in the process.

5. Hackerspaces and Makerspaces. Honestly, what's not to love about these names? They just sound cool. And they are! Hackerspaces and Makerspaces refer to meetups in your local area, allowing you to meet

people, tinker around, pull cool knobs, and push funky buttons. Also, members often give presentations in a show-and-tell type of way, which provides you a great avenue to build and polish your presentation skills.

> *A word of advice: when you visit meetings like this in your area, take a pencil and notepad! I know, it feels a little old school, but everyone at the conference is there for the same reason--to meet people, play with cool things and get contact info. We promise it doesn't feel awkward or weird to write this down. In fact, most people are flattered that you'd even want their info. Take our word for it--you'll want a way to follow up with people and send your resume to share with others, and a pencil and notepad is just the ticket.*

Once you have a couple of these events behind you, your network will start to grow. Word of mouth, remember! But we can't leave networking without one last recommendation--

Use those traditional job posting boards, too.

Applying for Jobs

Alright, here we go. It's almost time to look for that job. A key element before that is a polished resume--it takes time and effort, but it's a vital vehicle that will take you to your next destination in style.

All resumes have the same basic information, even if they take different forms. Let's look at each necessary section.

- **Contact Information.** This is pretty standard. You'll need the following:
  - **Full name.** If your name is difficult to pronounce, employers may find it more inviting if you include a pronunciation guide or give your nickname in parenthesis. You can also consider using Ms. or Mr. before your name.
  - ***Email.*** You'll want to use a professional email address on your resume. In other words, if you're still using something like fuzzybunny@aol.com or fridaynightlightsYEET@yahoo.com, it's time to update your email address service provider and your username. Keep it simple and professional, like john.doe@gmail.com or jdoe@icloud.com.
  - **Phone number.** These days, very few people have home phones, but we all likely have smartphones. Since cell phones are how most people communicate, you need to include it on your resume. Be sure your voicemail greeting is professional.
  - **Address.** 40% of employers use applicant tracking systems (ATS) to screen candidates. ATSs look for key terms, and your address is one of those. If you leave it off, you might put yourself out of the running for a job.

- **LinkedIn profile.** If you don't have one, get one. It gives an overview of you as a professional and allows you to include more information than a concise resume. Including your profile link allows you to give the hiring manager more personalized information about yourself. Polish it, customize your URL, and include it as a hyperlink in your resume contact section. Trust us on this one.

• **Summary.** This section allows the hiring manager to quickly identify your strengths to determine if you're a good fit for the role. In IT, a summary might look something like this:

> *Dedicated and friendly IT consultant with over six years experience in a fast-paced start-up company. Eager to offer excellent analytical skills to help XYZ Inc. grow their customer base. Recognized in previous roles for company-wide satisfaction rating (over 97%). Client satisfaction boosted by more than 35% over one quarter and client wait time reduced by 18%.*

• **Education.** Any formal education and certifications need to be on your resume. If you have degrees that aren't related to technology, list them anyway. But if you have unrelated certifications, leave them off.

• **Skills:** Your skills should line up with the position you're applying for. Areas to include are technical skills, leadership skills, interpersonal skills, soft skills, and problem-solving skills.

• **Job Experience:** Your previous job-related experience should be included here, and if you can, connect that to the role you're applying for. Use strong action verbs like established, spearheaded, and produced. Some hiring managers recommend only going back five years or two pages, whichever comes first; use your discretion here.

• **Objective**: This is an optional section but one we recommend. An objective refers to a short, targeted statement that reveals your career direction and positions you as a candidate who fits the job. When done well, it adds value and sets you apart from the crowd of applicants. Here's an example:

> *Reliable and enthusiastic professional who's interested in a Security Analyst position with DEF company; able to apply analytical, technical, and innovation skills to support and guard organizations against security breaches.*

Once you've polished that resume, you're ready to job search!

Job Sites and Job Titles for the Win

Alright, alright, alright!

Your resume is looking good. You're gearing up for locating that perfect job.

Now what?

First, you may find success on several job posting websites, and we definitely recommend spending some time there: Indeed, Zip Recruiter, and Glassdoor are a few places to start your search.

Next, consider a premium membership on LinkedIn, which shows the statistics for each job you apply for, sends messages to hiring managers for companies you're interested in, and reveals who's looking at your profile. If it fits in your budget, it's a no-brainer.

Finally, put Google to work for your job search, too, by setting up and configuring job alerts.

How to set up those alerts, though? You'll need the right job titles:

- Security analyst
- Information security analyst
- Security Operations Center (SOC) analyst

Ok, this calls for a moment of transparency. While the SOC might be the lowest paid of the three job titles above, to get your foot in the door, you want to consider a temporary pay cut and remember that the trajectory of salaries is steep.

After all, a security analyst position is the easiest to land because it's usually a revolving door, and these positions open frequently.

Over time, many senior security analysts make well into the six-figure range, which is just one step up from an SOC analyst. Not two or three steps away--juuust one.

So keep your eyes on the prize and be willing to sacrifice a little in the beginning. You won't regret it!

Now you've got a great resume. You've learned the proper job titles for searching, and you've been applying for jobs left and right. Let's imagine you made it to an interview--a whole new beast! Don't worry. We've got you.

Common Interview Questions

Here, we're sharing common interview questions for a junior SOC analyst, so spend some time on these to be well-prepared when it comes time for that coveted interview.

1. What is an RFC1918 address? Do you know them?
2. Define a Class A, B, or C network.
3. What are the seven phases of the cyber kill chain?
4. What is the purpose of the Mitre ATT&CK Framework?

5. What's the difference between TCP and UDP?
6. What are the ports 80, 443, 22, 23, 25, and 53?
7. What is data exfiltration? What Windows protocol is commonly used for data exfiltration?
8. Do you have a home lab? Describe it.
9. What is AWS? Explain how you've used it
10. What is a DMZ, and why is it a common target for cyberattacks?

Depending on your background, these questions may feel simple to you. But realize that 7 of 10 candidates don't know many of the answers.

That won't be you, though, because you have a chance to practice ahead of time. Be sure you know these questions and answers like the back of your hand. Or the front of your keyboard.

Though you'll need technical knowledge, that makes up just half the requirements for an SOC analyst. You'll also need to be a critical thinker and possess an acumen for problem-solving. Interviewers will often identify this by asking scenario-based questions.

Tips for a Killer Interview

To become the best applicant out of all the candidates, keep these tips in mind:

- Dress professionally. You only get one chance for a first impression! Ask about the dress code ahead of time. It makes interviewers feel more comfortable when you are dressed per company culture. Discussions tend to be more aligned with how you'd expect your day-to-day life at the company would be like.
- Bring your resume and provide a copy for each interviewer (including yourself).
- Be organized and prepared to take notes. If you can afford a portfolio, which is essentially just a case for a legal pad, carry one with you into the interview. I personally have a black and brown one to match my belt and shoes.
- Use active listening techniques during the interview. For example, allow the interviewer to finish talking before replying. Nod your head, and lean in. Use brief affirmations like "I see" or "I agree."
- Be aware of your body language.
    - Walk confidently from the waiting room to the interview room.
    - Make eye contact--and keep it.
    - Sit up straight and avoid crossing your arms.
    - Avoid signs of restlessness like tapping the table or kicking your foot back and forth.

- Prepare questions about the role, the company, and growth opportunities. There may be several interviews with different people in various positions and it is OK to reuse questions. You might get different answers. Typical questions might include, for example:
    - Is this a new position, or who was previously in this role, and what happened?
    - What are the challenges and expectations in the first 30 and 90 days?
    - What would you consider to be success in this role?
    - Does the company support their employees volunteering in local STEM programs?
    - How does this position progress in the company?
- Ask for feedback and next steps at the end of the interview.
    - To improve my interviewing skills, can you provide any positive or negative feedback? - This shows that you are invested in growing as a professional and gives insight into how the interview went.
    - What are the next steps in the interview process? - You may feel uncomfortable at first asking this question but do it. Trust me on this

Chapter 3 Quiz

1. For an online community of support in the hacker culture that includes meetup spaces and a magazine, check out _____.

a. 2600.org
b. Def Con
c. BSides
d. OWASP

2. This conference meets in Las Vegas each year and draws recruiters looking for qualified IT professionals.

a. BSides
b. OWASP
c. Def Con
d. Hackerspaces

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

a. Def Con
b. OWASP
c. BSides
d. 2006

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

a. Unrelated certifications
b. Experience related to IT
c. Skills that line up to the job listing
d. Phone and email address

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

a. Information security analyst
b. Security Operations Center analyst
c. Security analyst
d. Software analyst

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

a. LinkedIn provides an overview of you as a professional
b. LinkedIn enables you to upload multiple pictures of yourself

c. LinkedIn gives personalized information about yourself
d. LinkedIn allows you to provide more information about yourself

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

a. What's the difference between TCP and UDP?
b. What are the ports 80, 443, 22, 23, 25, and 53?
c. What's an RFC1928 address?
d. What is a DMZ, and why is it a common target for cyberattacks?

8. Which of the following was not on the list of questions you might be asked in an SOC analyst interview?

a. What is ASW?
b. Define a Class A, B, or C network.
c. What are the seven phases of the cyber kill chain?
d. What's the purpose of the Mitre ATT&CK Framework?

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

a. Use brief affirmations like "I see"
b. Make eye contact
c. Maintain good posture
d. Avoid signs of r estlessness or boredom

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

a. Indeed
b. Monster
c. LinkedIn
d. Glassdoor

PREREQUISITE SKILLS



You've got 99 problems but a skill ain't one!

In this chapter, we'll make sure this is true by talking about the skills needed to land your first cybersecurity job.

First, though, I want to be clear that while we can't teach you everything you need to know, we will cover the fundamentals based on a common baseline of knowledge which rests on network and security fundamentals. This type of prereq knowledge can be learned through formal security certifications like CompTIA Network+ and Security+.

Let's get started by going over the concepts you'll need to know to crush an interview, starting with our good ol' reliable friend, networking.

Networking

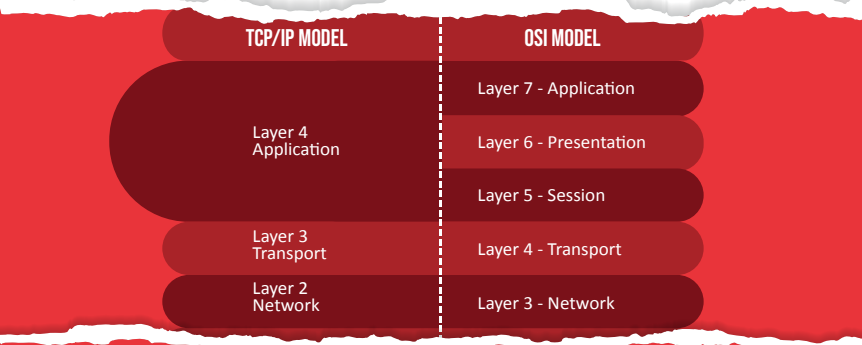
This section isn't about talking to people; instead, we're covering the basics of the modern TCP/IP stack.

The Transmission Control Protocol and Internet Protocol (TCP/IP) was created in the 1970s by DARPA scientists, Vinton Cerf and Bob Kahn. At that time, no standardized network standard existed, but after a decade of tests and refinement, the TCP/IP stack was launched in 1983.

Soon, the US Department of Defense adopted it, securing TCP/IP as the standard moving forward.

The TCP/IP stack consists of four layers, each one solving a set of problems around data transmission. This is where the magic happens. If you need to send a file or email, the TCP/IP stack goes to work for you.

Alternatively, there's a seven-layer model called the Open Systems Interconnection (OSI) model. OSI is generally used more because it provides a more granular view of the encapsulation process. Moving forward, we'll use the OSI model. Let's take a quick look at both for comparison:



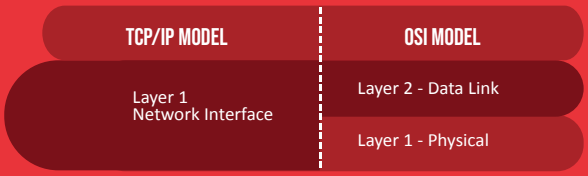


FIGURE 4-1: TCP/IP AND OSI MODEL

If you're curious to learn more, search YouTube for "OSI Model Encapsulation" to discover informative videos breaking down the process through animation for easier understanding.

Let's talk about IP addresses now. There are two types:

- IPv4 (10.0.0.1) is the previous standard of how machines on the internet communicate with each other. While 4 billion addresses seemed like plenty at one time, the increasing Internet landscape means we've started running out of 32-bit IPv4 addresses.
- IPv6 (2001:0db8:85a3:0000:0000:8a2e:0370:7334) is the updated standard for identifying computers on the Internet. It also provides a unique identifier but has been adjusted to 128-bit.

There are also two type of network spaces:

- Public, a network that is accessible to the public internet. Generally leased by an Internet Service Provider (ISP).
- Private, a network that is owned and managed by an individual or organization.

Using networking devices, people typically have one public IP address that is the single point of access to the broader public internet for the many internet connected things in your home. However, organizations typically need many public IP addresses so that people and other organizations on the broader internet can access their services.

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

FIGURE 4-2: RFC 1918 ADDRESSES

Beyond the RFC1918 address space, you'll want to know the common port numbers and differences between TCP and UDP.

- TCP relies on an established connection called a three-way handshake and UDP protocol. If a piece of data is missed in transit, TCP will resend the missed packet and put the packets back in order. TCP connections are used when every bit of data needs to arrive at the destination, like a file transfer. Without all bits and bytes, a file can't run.
- UDP sends messages and doesn't care if they get there or not. We often jokingly call it "Unreliable Dang Protocol" for this reason. UDP is often used for video streaming.

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

FIGURE 4-3: COMMON PORT NUMBERS

Another item to address is the three-way handshake. Let's try to break this down in an easy-to-understand way:

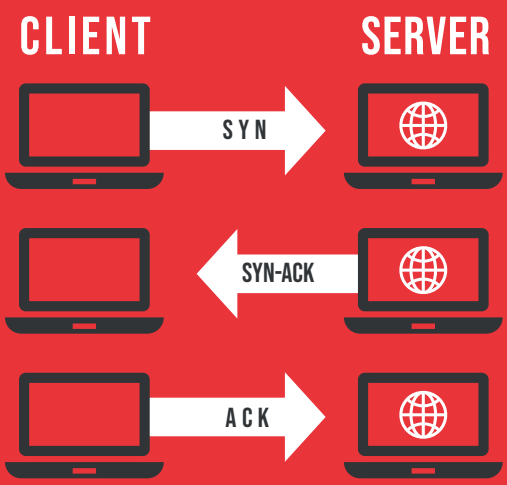


FIGURE 4-4: THREE-WAY HANDSHAKE

- Let's say you're uploading a file to an image hosting website.
- Your computer first establishes a connection to the server by sending an SYN packet.
- The server then sends a SYN and Acknowledge packet back.
- The client sends the Acknowledge packet back.
- The three-way handshake is now complete.

This process will matter in your new SOC analyst job if, say, a host on the public Internet attacks your network's perimeter. You may only see a SYN packet, which sometimes occurs if firewalls drop it because it's not approved traffic.

But if you suspect a computer on your network is communicating with a malicious host and the handshake process has been completed, it's likely they have actively communicated, and some data may have been transferred.

With the basics of networking established, let's move on to related security.

Network Security

When we refer to CIA related to cybersecurity, we are talking about Confidentiality, Integrity, and Availability. All security can be broken down from these three high-level categories:

1. Confidentiality refers to the secrecy of information, making sure that only the intended people can see the information.
2. Integrity refers to the correctness of the data, ensuring you're only consuming data that you intend to, and that the data is complete and unaltered.
3. Availability ensures the data can be used when needed.

Other vital terms related to the basic tenets of security include:

- Firewalls ensure that network resources are only accessed by approved individuals.
- Access control lists (ACLs) ensure the general internet can't access private networks. ACLs act as confidentiality controls and availability controls.
- Network perimeters are boundaries between public Internet space and RPC1918 private Internet space. Perimeters are set by networking appliances.
- Least privilege is a concept related to access control models that says no one needs more access than the absolute minimum needed.
- Separation of duties refers to important duties being separated to provide less opportunity for fraud.

Cryptography

When we say cryptography, we're referring to a method of storing and transmitting data so that only the audience it's intended for can read and process it.

Cryptography principles require you to know the difference between encryption and hashing:

- Encryption refers to changing data in a way that makes it unreadable with the intent that the data will be changed back to a readable state.
- Hashing takes a set of data and creates a unique fingerprint from it.

The main difference between encryption and hashing is that a hash is one way; there's no viable way to turn the unique string of characters, or the fingerprint, back into the original characters.

Endpoint Security

90% of all malware infections come from emails. Networking and network security are important, but the front lines of the cybersecurity war are fought at your network endpoints.

Targeted devices include laptops, smartphones, and printers, to name a few. Because there are so many devices on the market, endpoint security is a challenge.

The most valuable skill here will be understanding how each operating system can be exploited or compromised. The three most common are Windows, Unix, and MacOS.

- Our first OS, Windows, is the global market leader for user endpoints. In fact, 87% of all companies run some version of Windows. Even though newer iterations exist, many older versions are still used. Unfortunately, older Windows OSs aren't maintained when newer ones are released, meaning zero security patches or help desk support. In fact, about 30% of all Windows users are using a version that's no longer supported, opening up many targetable systems for cyber criminals and script kiddies around the world. Windows is often targeted in the following ways:

    1. Phishing: users unknowingly open fraudulent links or attachments that reveal personal and sensitive information.

    2. Weak passwords: users choosing passwords that are easy to guess is the culprit here. Don't use passwords that could be guessed by googling your name or business. Also, using words in password makes them easier to guess. Instead, create longer passwords with a diversified character set to deter hackers.

        To learn to crack passwords as a cybersecurity professional, consider learning tools like John the Ripper and Hashcat, but do not steal or attempt to log in to services with other people's passwords. You may not attempt any hacking activity without expressed or written permission.

    3. User permissions: most at-home users act as the local administrator of their endpoint, which is acceptable in a home setup. In a company, though, allowing the workforce to operate as the local administrator for their endpoints means the risk of malware infection is significantly higher.

- Our next OS, MacOS, is being adopted by more and more companies as their endpoints of choice, making it the second most popular OS in the world. MacOS is a proprietary flavor of Unix, allowing the OS to operate on lower system resources and provide greater user control. Apple owns around 10% of the OS market share, which doesn't sound like a lot but translates to millions and millions of users.

Apple is more secure because it's taken endpoint security to the hardware layer with built-in security chips on the motherboard. These chips encrypt the file storage, ensure a secure boot of the OS every time, and provide application runtime security. Apple's proprietary operating system means that malware authors must tailor their attacks specifically for apple devices which is becoming more common, but overall MacOS has less malware attempts.

Apple's MacOS is a great option for increased security in an enterprise environment, but it usually calls for a high level of IT support and can be expensive.

- Our third OS, Unix/Linux, continues to grow in popularity, owning around 2% of the market share and possessing many different versions. With the advent of the Internet of Things or IoT (which refers to a networking capability that allows information to be sent from objects and devices using the Internet, like a kitchen appliance or fixture in your home), Unix/Linux has infiltrated their way into just about every home and office in some way.

Most Unix/Linux Oss are compromised through misconfigurations in either the OS or the applications hosted on the system rather than malware, which does exist but isn't widespread.

When it comes to endpoints, Unix/Linux users haven't adopted it as a personal OS because of the difficulty in managing it. Linux is used more often as an endpoint OS in cybersecurity and software development communities.

- Other Endpoints we should cover include mobile devices, tablets, and cars with built-in Wi-Fi hotspots. For these operating systems, Android, iOS, and Linux are popular.

  Next, as we discussed earlier, IoT devices include many smart devices you may already have in your home. This biggest risk for these devices is an attack called "credential stuffing" which

a threat actor reuses old passwords found in leaked databases from previous hacks to access your IOT management portal.

Finally, the Chromebook by Google is a low-cost solution for a laptop and touts itself as the most secure OS on the market. Remember, though, that a system is only as secure as the apps it has installed. Google does try to limit these, but there are methods that can circumvent these protections.

Chapter 4 Quiz

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

a. It's made up of seven layers
b. The US Department of Defense adopted it
c. It's made up of four layers
d. It was launched in 1983

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

a. Ipv6, Ipv4
b. Ipv6, Ipv8
c. Ipv2, Ipv6
d. Ipv4, Ipv6

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

a. two-way handshake
b. three-way handshake
c. UDP
d. encryption

4. _____ create the bou ndaries of a network and_____ ensure the general Internet can't access private networks.

a. Firewalls, access control lists
b. Access control lists, firewalls
c. Firewalls, least privileges
d. Access control lists, network perimeters

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

a. Hashing, encryption
b. Encryption, hashing
c. Perimeters, hashing
d. Encryption, perimeters

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

e. MacOS
f. Unix/Linux
g. Windows
h. Debian

7. Which of the following does not properly represent Oss and their market share?

a. MacOS, 10%
b. Windows, 87%
c. Unix/Linux, 2%
d. Unix/Linux, 10%

THE SOC ANALYST



Security. It's a big deal!

Come along with Tyler as he describes working as an SOC analyst to give you an insider view of how serious security is taken in an SOC. He's arrived at work and entering the company:

> *I badge in at the front door of my office building and greet the security guard who's there every day. From there, I head to the elevator for my floor, where my badge is needed once again to unlock it. Now on the SOC floor, I use my badge one more time to get to the common areas. This is where the sales and engineering teams sit, too. As I approach the center of the room, I see two doors within feet of each other. We call this area the "mantrap", which allows security to trap someone between the two doors and escort them out of the building, if needed. I swipe my badge at the first door, which lets me in, and as always, I fight a tiny bit of anxiety that I might get stuck between the doors. My badge opens the second door, though, and now I'm in the heart of security: the SOC. There are windows, but they're covered with blinds, making it dark. Looking up, I see TVs lining the ceiling which display what's going on in our global company and across the world in real time. I'm immediately sucked into my role, and after greeting my coworkers, I jump excitedly into my job.*

Sounds top-secret and oh-so-cool, right?

Let's point our attention to the tools in an SOC.

Tools of the Trade

As a security analyst in the 2020s, you must know about **Security Incident and Event Management (SIEM)**, which provides a real-time analysis of security alerts before they have a chance to disrupt business operations. SIEM means security specialists can look at their network through a larger lens, merging together security controls and infrastructure.

SIEM is the heartbeat of every SOC! Everything that's done on a device can generate a log, and without a log, there would be no security and no security analysts.

In fact, SOCs all over the world generate logs with the idea of sending them to a single point where the logs can be observed and measured. We refer to this concept as a "single pane of glass," ideally one screen that the SOC can operate without having to chain together multiple web browsers and sites to review security events.

In this description, the single pane of glass is the SIEM, so let's learn more about SIEM and other tools.

- SEIM completes the following tasks:
    - Normalizes logs and puts them in chronological order
    - Accounts for all logs and ensures they're in a the proper format
    - Creates rules that will sound an alarm if any logs match the given criteria

SIEM is working toward taking on the following tasks in the future:

- Acting as case managers by combining and tracking multiple alarms for investigations in a way that's meaningful and easy to use
- Automating integration through **Security Orchestration, Automation, and Response (SOAR)**, which allows predefined playbooks to run automatically for common security issues, freeing up staff to work on more challenging and interesting items

Examples of SIEM are Splunk, Elastic, LogRhythm, Qradar, FortiSIEM.

- Firewalls. In addition to SIEM and SOAR, firewall and firewall engineering are a specialty of their own. You'll want to be familiar with the big players in the firewall space, including Cisco, Checkpoint, Fortinet, Palo Alto, Juniper, and SonicWall.

  As an SOC analyst, you might be asked to perform a firewall block on an IP address. Part of your job will likely include using the appropriate tools and techniques to determine if something is wrong and then blocking that IP address from communicating with your internal network.

- Intrusion Prevention System/ Intrusion Detection System (IPS/IDS) provides protection and detection. Most IPSs can act as IDSs and vice versa, but the main difference is their location on the network. They might be host-based or network-based, and they may be referred to as HIPS/HIDS or NIPS/NIDS. Together, these are known as intrusion detection and prevention systems (IDPS).
    - The protection system, IPS, allows a device to take action as needed to control the flow of network activity. Placing an IPS in line allows it to control the progress of traffic and take preventative actions when needed.
    - The detection system, IDS, only allows for detection, not any interjection or intervention. Tapping the network allows the device to see the network traffic but not affect bandwidth.



INTRUSION DETECTION SYSTEM

Intrusion Detection Systems can either be placed in line or through a network tap as seen here. intrusion detection systems are designed to detect and not take preventative measures.

Tapping the network allows the device to see the network traffic but not affect bandwidth. IDS placed through a tap can not take preventative action because they can not control the flow of traffic.

FIGURE 5-1: INTRUSION DETECTION SYSTEM



INTRUSION DETECTION SYSTEM

Intrusion prevention systems must be placed in line as seen here. Placing an IPS in line allows it to control the flow of traffic and take preventative actions to protect.

IDS can be placed in line as well. Most modern IPS will have some rules set to take action and some set to monitor only. These are called Intrusion Detection and Prevention System (IDPS).

FIGURE 5-2: INTRUSION PREVENTION SYSTEM

- Sandboxing refers to executing the file or website in a protected environment to find out what it does. Endpoint detection software will detonate a file on your behalf, but even better is to use reports from Cuckoo, Hybrid Analysis, or Joe Sandbox. These tools will press every button and twist every knob to get execution information from a file. Other online tools for sandboxing include:
    - **Virustotal.com:** perhaps the most useful; put in a URL or hash to test it
    - **Domain Tools:** offers the whois tool, which is very easy to use

- **Talos Intelligence:** conducts reputational checks on IP addresses and URLs
- **IPVoid:** checks blacklists for a particular IP address
- **URLVoid:** checks URLs for safety reputations
- **Threat Crowd:** acts as search engine for threats and finds and researches artifacts related to cyber threats
- **TOR Exit Node List:** checks if the IP address is on a TOR exit node
- **IBM X-Force Exchange:** checks the IoC for information in X-Force Exchange
- **Search Engine:** checks a search engine for hiding suspicious items

As an important note, the value of a search engine like Google cannot be understated. Google may bring up something helpful that an SOC analyst never would've found if not for that search, so always keep that in your toolkit.

Definitions

Since cybersecurity terms often have vague meanings and aren't always agreed upon, let's specifically look at these crucial elements and how often they occur for your benefit.



FIGURE 5-2: FUNNEL CHART

- **MOST COMMON:**
  - Security logs are the base of a security program. In your future job, you would want to capture logs like network flow, Windows Events, Unix Syslogs, and firewalls.
- **COMMON:**
  - Security events refer to the day-to-day routine security monitoring from tooling. Almost all security tooling notifications start as a security event generated from security logs. A security event must be escalated to a security incident before becoming a breach. The incident response then triggers the process of assigning an incident handler.
- **UNCOMMON:**
  - Incidents occur more often than a security breach. Once an incident is declared, the incident response process begins if there is suspected loss of sensitive data. Events that are not considered incidents are security events and vulnerabilities that haven't been escalated.
- **RARE:**
  - Security breaches contain a verified loss of data containing sensitive personal information. Breaches often require the legal department and CISO to declare a breach. Breaches start as incidents, require notification to clients and maybe the public, and are handled with careful sensitivity.
  - In your future career, it's advised not to use this term unless told otherwise!

Chapter 5 Quiz

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

a. SIEM
b. IPS
c. IDS
d. SOAR

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

a. SIEM
b. SOAR
c. UEBA
d. IPS

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

a. UEBA
b. SIEM
c. IDS
d. SOAR

4. Common firewall options include all the following except:

a. Super Sonic
b. Cisco
c. Checkpoint
d. Palo Alto

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

a. IDS
b. IPS
c. SOAR
d. SIEM

6. _____ allows for detection, not intervention.

a. IDS
b. IPS
c. SIEM
d. UEBA

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

a. shadow boxing
b. encryption
c. sandboxing
d. an incident

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

a. Incident
b. Breach
c. Security event
d. FIRE

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

a. Incidents
b. Breaches
c. Events
d. Logs

10. All the following are sandboxing tools except:

a. Talos Intelligence
b. URLVoid
c. Threat Crowd
d. Juniper

SOC
IN THE CLOUDS



What is Cloud Computing?

Cloud computing has a complex and formal definition but let's look at a simplified version for ease in understanding.

Overall, **cloud computing** provides an operating model to deliver services like computing, storage, network, databases, platforms, and applications. It does so by using a service model on top of the usual data center's basic building blocks. Cloud computing allows for various levels of rapid deployment of these services through the internet.

If the hardware is managed and owned by an internal IT team it is known as a **private cloud**. If a company outsources all the management of the cloud infrastructure, it is a public cloud. Otherwise, a combination of both is a **hybrid cloud.**

The most common **cloud service providers (CSP)** are: AWS, Google GCP, or Microsoft Azure. These companies establish and manage private clouds.

Fast Facts

- **Public cloud**
  - Owned by: Cloud providers like AWS, Google GCP, or Microsoft Azure
  - Consumed by: Enterprises and individuals using a pay-as-you-go billing model
  - Responsible for: Managing, maintaining, and developing the computing resources pool shared between various clients
- **Private cloud**
  - Owned by: An enterprise that offers infrastructure and application platforms to internal consumers or developers
  - Consumed by: A single organization
  - Works by: Giving complete control to the company and scaling resources up and down as required
- **Hybrid cloud**
  - Defined as: A combination of public cloud and private cloud. A private cloud is always involved.
- **Multicloud**
  - Defined as: A cloud deployment model consisting of multiple clouds--private, public, or both.

Cloud Service Models

Moving forward, you'll want to be familiar with the four cloud service models that are most popular.

- **Infrastructure as a Service (IaaS).** IaaS refers to a public or private cloud deployment that's used to offer infrastructure components like:
  - Servers and storage
  - Networking hardware
  - The physical data center itself
- **Platform as a Service (PaaS).** PaaS refers to a kind of development platform that's used to deploy binaries and develop data applications or stores
  - Examples:
    - Google App engine--public, code deployment
    - AWS Elastic Beanstalk--public, code deployment
    - Azure App Service--public, code deployment
    - Heroku--public, code deployment
    - Cloud Foundry--private, code deployment
    - AWS Redshift--public, data mart development
- **Desktop as a Service (DaaS or IaaS + PaaS).** DaaS delivers managed virtual desktop infrastructure (VDI) as a service over the network.
  - Examples:
    - AWS Workspaces
    - Microsoft Azure DaaS
    - VMware
    - Horizon Cloud
    - Citrix Managed Desktops
- **Software as a Service (SaaS).** SaaS delivers software that's accessed online and usually through a subscription. It offers fully executed applications instead of development building blocks like IaaS or PaaS.
  - Examples:
    - Salesforce for CRM
    - Workday for HCM
    - Microsoft Office 365 for office productivity suite

Cloud Security

If you haven't heard this phrase yet, you'll be familiar with it before long:

> The provider is responsible for the security of the cloud, and the consumer is responsible for the security in the cloud.

This general rule of thumb provides valuable insight into the fundamentals of cloud cybersecurity.

There are clear boundaries in responsibility for cloud security. Consider this graphic, shared earlier and now overlaid with who's responsible for what:

Chapter 6 Quiz

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

a. private
b. public
c. multicloud
d. popular

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

a. private
b. multicloud
c. hybrid
d. public

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

a. secret
b. hybrid
c. compound
d. outcross

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

a. tri-cloud
b. auxiliary-cloud
c. common cloud
d. multicloud

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

a. hypervisor
b. hypovisor
c. inner visor
d. output visor

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

a. of, in
b. in, of
c. before, after
d. between, around

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

a. Software as a Service offers developmental building blocks
b. Platform as a Service is used to deploy binaries and develop data application or stores
c. Desktop as a Service delivers virtual desktop management over the network
d. Infrastructure as a Service is deployment that uses infrastructure components like computing, storage, and network devices.

SOC AUTOMATION



When we refer to automation in SOC, we're talking about:

- **Security Automation and Orchestration (SAO) or**
- **Security Automation, Orchestration, and Response (SOAR)**

And as an SOC analyst, you're likely to encounter some type of security automation within an organization. Let's dive into maturity models to learn how those relate to automation.

First, though, let's define security automation.

What is SOC Automation?

Simply stated, **automation** is the machine implementation of low-level security-related actions, which are smaller pieces of a larger task.

A **task** is made of a number of actions that are partially or fully automated. Their goal is to reduce human intervention in security operations.

From there, a **process** encompasses a number of tasks.

Orchestration is closely tied to automation, but it takes advantage of multiple automation tasks across multiple systems or platforms. Additionally, orchestration is used to automate or semi-automate more complex workflows and processes.

Now, some SOC analysts and others in the security community criticize automation. They seem mostly concerned that automation will take their job. I mean, if a machine can do it faster and more efficiently, what's an analyst to do?!

Let me present it like this. *Automation should be a springboard to an SOC analyst, not a limitation or replacement.*

We want analysts to continue detailing events, which takes a great deal of time and just isn't possible with the numbers of events coming in daily. Additionally, we need SOC analysts to look for trends, examine data over time, and find reasons the events are occurring. They should ask themselves, "Is the reason I have to respond to 50 events per day because the web server is vulnerable?" They should take that information to their SOC leadership and show initiative to patch the vulnerability.

Automation is a positive addition for any SOC. Let's look at why

Why Automate?

SOC analysts are incredibly valuable resources who will always be needed to perform jobs that machines simply cannot.

Think of it this way. SOC leadership is often tasked with new requirements and additional services--but with the same (or fewer!) resources. They're being pressured to deliver more, and combined with a shortage of skilled cybersecurity professionals, automation becomes more appealing and necessary.

You can see where this is going. Automation helps analysts with the flood of events coming on a daily basis.

Imagine how automation can free up **analysts** from monotonous tasks. They can instead spend more time on higher-level analysis of events. In addition, senior analysts can spend more time training junior analysts.

Consider, too, that automation can streamline existing processes.

For one, automation reduces analyst fatigue. For the amount of day-in and day-out information that must be collected, categorized, analyzed, and interpreted by an SOC analyst, it's easy to see why analysts start to feel brain-fried. By relieving this fatigue and stress, the SOC is a more challenging and fun place to work. With that in mind, automation can promote morale and create a healthy workplace environment.

The second reason for automation is to **reduce mistakes**. It's easy for analysts to make errors during the constant document checking and console switching. By automating these tasks, the likelihood of mistakes is far less. And it also increases consistency, which is key in security operations.

A third reason to automate is to **reduce information bias**. Analysts may create false positives or take off down a rabbit hole. Unfortunately, it's simple for one wrong attribution to skew a full dataset. Automation, therefore, ensures consistency.

Finally, automation allows operations to **keep up with the speed at which attackers** are evolving. Every few months, there seems to be a new attack pattern with more complex threats. Automation and orchestration can help reduce the mean time to detection **(MTTD)** and **mean time to response (MTTR)**. These can save time that adds up and leads to significant time savings.

Metrics decreasing will also satisfy senior management, and happy senior management is always a good thing.

SOC Maturity

Truly, there's no way to automate all processes in an organization, which simply gives you job security.

There are just too many situations when a real-life analyst is needed. Automation has led to horror stories in the past, leading to catastrophic effects on businesses--and their reputations.

As such, there must be checks and balances in the automation process. And those measures require human interaction and approval before being implemented.

Now, the topic of this chapter is SOC Maturity, so let's get to it. Or at least a shallow dive into determining an SOC's maturity.

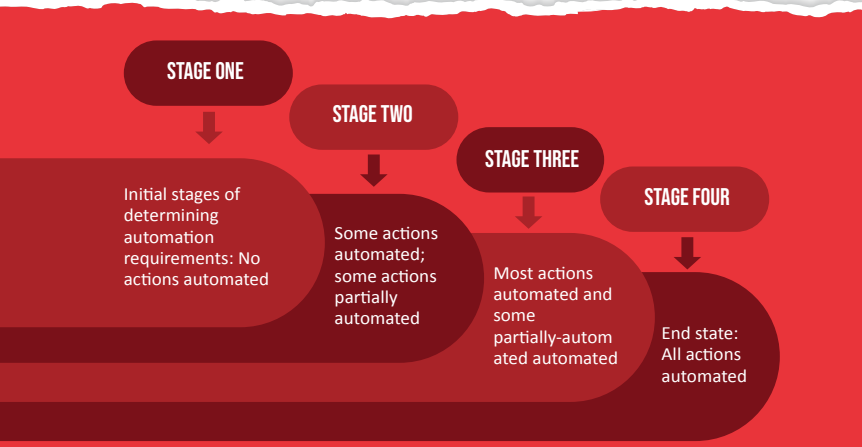


FIGURE 7-1: AUTOMATION STAGES

As shown in figure 7-1, you can begin with a staged approach to assess the maturity of an SOC's automation. You can see that once you've completed an inventory of your SOC today, then you can map your current state and measure your progress toward established goals.

You can start with small goals. And you can start anytime. Just start! Because automating actions gets you closer to your goals.

Now, as a junior analyst, you'll start to see areas for improvement in the processes used by you and your team every day. Keep an eye out for gaps, and look for actions that can be automated. Take your time and gather the proper data. Then do an analysis.

Ask yourself, can any of these actions be automated? What benefits do you see it providing to the team?

Being able to articulate process improvements or resolutions will set you up as a leader among your colleagues. Additionally, SOC leadership will view you as a real deal problem solver.

That right there is worth its weight in gold.

How to Start Automating

As with most things, there really isn't a one-size-fits-all approach. Here are our recommendations:

1. Someone who is intimately familiar with the organization's processes and procedures should spend some time analyzing the work they do each day. Before long, this will be you!
2. Categorize the tasks by the amount of time they take. Focus on the simple tasks because automating them can make a sizable amount of progress. Check out Figure 7-2.

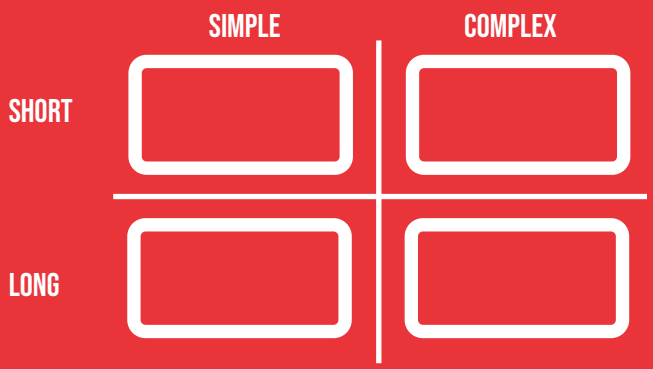


FIGURE 7-2: AUTOMATION MATRIX

3. Now, look for repetitive actions with complex conditions. Make every effort to break it down into the smallest possible steps.

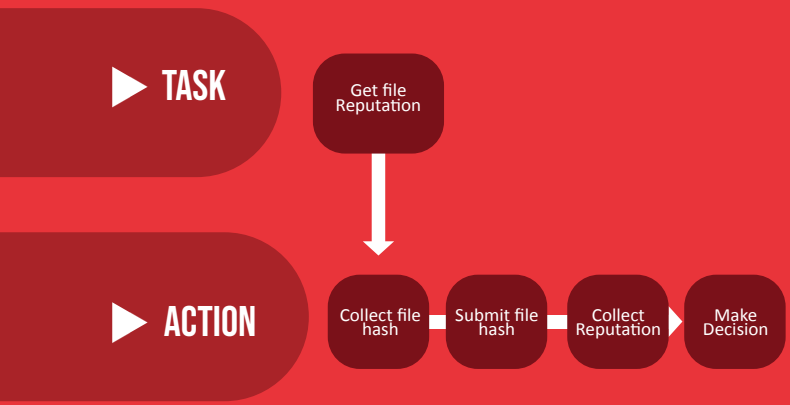


FIGURE 7-3: GET FILE REPUTATION

Review Figure 7-3. Let me break down the tasks for you as a future analyst:

a. Gather the file hash.
b. Open a web browser.
c. Paste the hash into the browser and submit it.
d. Make a decision based upon the file reputation

The decision made upon the file reputation might then feed another action or process flow further downstream.

A playbook can be this small, and it's also possible to have a playbook that calls other playbooks synchronously, waiting for the first one to complete before calling another.

I know. It may not look like much time will be saved by automating this task. But it sure might reduce the number of tickets you respond to! *SCORE.*

Sample Use Cases

Part of the SOC automation journey is realizing that what works for other platforms might not work in your environment. That's to be expected.

Bearing this in mind, I'll share a couple of use cases that might act as a starting point for your future automation endeavors. They likely won't be an exact fit, but they're good scenarios to consider.

1. If you haven't already started your automation journey, talk with your team about the benefits.
2. Do a full inventory of the tasks your SOC performs.
3. Break them down into the time required and complexity demanded.
4. Define your use cases before automating any actions. Focus initially on tasks that are simple and fast, providing you some quick wins.
5. Don't write long, complex playbooks. As much as possible, break them down into specific tasks. Also remember the option to use a parent playbook to call multiple child playbooks.
6. Don't fear challenging the status quo. Beginning an automation process will often reveal a new and better way to do something. Allow automation a chance to show its value to your organization.

It's true that security automation is still in its infancy, but it can be implemented to improve your SOC's operations. Take the lead! Show your team that automation isn't a limitation but a force multiplier for everyone to become better analysts.

Chapter 7 Quiz

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

a. Automation
b. Robots
c. Process
d. Orchestration

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

a. Automation
b. Process
c. Orchestration
d. Inventory

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

a. process, task
b. task, process
c. process, response
d. response, task

4. All the following are true regarding automation except:

a. It will replace analysts in the next five years
b. It streamlines existing processes
c. It frees up analysts from monotonous tasks
d. It manages the flood of events coming in daily

5. All the following are reasons to implement automation except:

a. Reduce analyst fatigue
b. Reduce mistakes
c. Reduce information bias
d. Reduce productivity

6. Which of the following is true regarding how to start automating?

a. Start with complex changes
b. Someone who is intimately familiar with the organization's processes and procedure should analyze the work done each day
c. Categorize the tasks by how much time they take
d. Look for repetitive actions with complex conditions

7. All the following are true about playbooks except:

a. They can be small
b. They can call other playbooks synchronously
c. They're only used in fantasy football
d. They should not cause incorrect or damaging actions

8. In light of automation, why do we still need analysts? All the following apply except:

a. Analysts are needed to detail events
b. Analysts are like robots
c. Analysts are needed to look for trends
d. Analysts are needed to examine data over time

9. All the following are true about orchestration except:

a. It's closely tied to automation
b. It automates more complex workflows
c. It takes advantage of multiple automation tasks
d. It's the opposite of automation

10. All the following are tips for using automation as a security tool except:

a. Write long, complex playbooks
b. Do an inventory of the tasks performed by your SOC
c. Challenge the status quo
d. Focus on simple, quick actions

QUIZ ANSWERS

Chapter 1 Quiz Answers

Correct answers are marked with an asterisk.

1. Which of the following companies had 100 million consumer credit applications stolen in 2019?

e. American Express
f. Citibank
g. Chase
h. Capital One

2. SOC stands for _____.

e. Standard Operations Committee
f. Security Operations Center*
g. Security Operations Committee
h. Security Oasis Center

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

e. incident
f. matter
g. mistake
h. casualty

4. All the following are true about Digital Forensics and Incident Response teams except:

e. They offer support to the SOC
f. They often take over long-term investigations
g. They often have similar skills to SOC analysts
h. They aren't focused on legal requirements for digital forensics*

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

e. Having more qualified SOC applicants than open positions
f. Training a new SOC analyst and then losing them to another company
g. Dealing with analyst burnout
h. Staffing a 24/7/365 operation

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

e. Chase the moon
f. Follow the sun
g. Ignore the clock
h. Avoid UV rays

7. MSSP stands for _____.

e. Management Super Secure Provider
f. Managed Security Shield Producer
g. Management Safeguarded Shield Provider
h. Managed Security Services Provider*

8. All the following are true about MSSPs except:

e. They sell security solutions
f. They go deeply into the infrastructure to learn the ins and outs of a network
g. They have a more robust hierarchy
h. The CEO is the security guy

9. The authors of this course say it could take _____ to settle into a new SOC analyst role.

e. 60 days
f. Three months
g. Six months
h. one year

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

e. Emotional
f. Creative
g. Analytical
h. Abstract

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

e. highest
f. lowest
g. longest
h. maximum

Chapter 2 Quiz Answers

Correct answers are marked with an asterisk.

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

e. IAM*
f. Operations
g. Engineering
h. Architecture

2. The Threat Intelligence team does which of the following?

e. Takes over incidents from the SOC and conducts investigations on long and enduring incidents
f. Researches new threats to enhance detection, determines if they're dangerous, provides details to management and the SOC
g. Focuses on enforcing the best security practices and compliance controls while implementing new technology
h. Deploys, manages, and maintains security tools

3. Relating to responsibilities, the Digital Forensics and Incident Response Team does which of the following?

e. Focuses on enforcing the best security practices and compliance controls while implementing new technology
f. Deploys, manages, and maintains security tools
g. Researches new threats to enhance detection, determines if they're dangerous, and provides details to management and the SOC.
h. Takes over incidents from the SOC and conducts investigations on long and enduring incidents

4. Responsibilities of the Security Architecture team include which of the following?

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

5. The Security Engineering Team covers which of the following tasks?

e. Identifies, catalogs, and remediates new and existing vulnerabilities

f. Takes over incidents from the SOC and conducts investigations on long and enduring incidents
g. Deploys, manages, and maintains security tools
h. Researches new threats, determines if they're dangerous, and provides details to management

6. The Vulnerability Management team is responsible for which of the following?

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

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

e. SOC Director
f. SOC Manager
g. Chief Information Security Officer
h. Risk Management team

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

e. Director of Security Operations
f. Director of Threat Management
g. Director of IT Security
h. Director of Risk Management

9. Which of the following internal teams focuses on the worst-case scenario?

e. Risk Management
f. Governance and Compliance
g. Privacy and Legal
h. Digital Forensics and Incident Response

10. Pertaining to government agencies, the team you'll most likely come in contact with as an SOC analyst is _____.

e. Regulatory agencies
f. Law enforcement
g. Military
h. Intelligence

Chapter 3 Quiz Answers

Correct answers are marked with an asterisk.

1. For an online community of support in the hacker culture that includes meetup spaces and a magazine, check out _____.

e. 2600.org
f. Def Con
g. BSides
h. OWASP

2. This conference meets in Las Vegas each year and draws recruiters looking for qualified IT professionals.

e. BSides
f. OWASP
g. Def Con
h. Hackerspaces

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

e. Def Con
f. OWASP
g. BSides
h. 2006

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

e. Unrelated certifications
f. Experience related to IT
g. Skills that line up to the job listing
h. Phone and email addres

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

e. Information security analyst
f. Security Operations Center analyst
g. Security analyst
h. Software analyst

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

e. LinkedIn provides an overview of you as a professional
f. LinkedIn enables you to upload multiple pictures of yourself
g. LinkedIn gives personalized information about yourself
h. LinkedIn allows you to provide more information about yourself

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

e. What's the difference between TCP and UDP?
f. What are the ports 80, 443, 22, 23, 25, and 53?
g. What's an RFC1928 address?
h. What is a DMZ, and why is it a common target for cyberattacks?

8. Which of the following was not on the list of questions you might be asked in an SOC analyst interview?

e. What is ASW?
f. Define a Class A, B, or C network.
g. What are the seven phases of the cyber kill chain?
h. What's the purpose of the Mitre ATT&CK Framework?

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

e. Use brief affirmations like "I see"
f. Make eye contact
g. Maintain good posture
h. Avoid signs of restlessness or boredom

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

e. Indeed
f. Monster
g. LinkedIn
h. Glassdoor

Chapter 4 Quiz Answers

Correct answers are marked with an asterisk.

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

e. It's made up of seven layers
f. The US Department of Defense adopted it
g. It's made up of four layers
h. It was launched in 1983

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

e. Ipv6, Ipv4
f. Ipv6, Ipv8
g. Ipv2, Ipv6
h. Ipv4, Ipv6

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

i. two-way handshake
j. three-way handshake
k. UDP
l. encryption

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

e. Firewalls, access control lists
f. Access control lists, firewalls
g. Firewalls, least privileges
h. Access control lists, network perimeters

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

e. Hashing, encryptionx
f. Encryption, hashing
g. Perimeters, hashing
h. Encryption, perimeters

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

m. MacOS
n. Unix/Linux*
o. Windows
p. Debian

7. Which of the following does not properly represent Oss and their market share?

e. MacOS, 10%
f. Windows, 87%
g. Unix/Linux, 2%
h. Unix/Linux, 10%*

Chapter 5 Quiz Answers

Correct answers are marked with an asterisk.

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

e. SIEM
f. IPS
g. IDS
h. SOAR

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

e. SIEM
f. SOAR
g. UEBA
h. IPS

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

e. UEBA
f. SIEM
g. IDS
h. SOAR

4. Common firewall options include all the following except:

e. Super Sonic
f. Cisco
g. Checkpoint
h. Palo Alto

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

e. IDS
f. IPS
g. SOAR
h. SIEM

6. _____ allows for detection, not intervention.

e. IDS
f. IPS
g. SIEM
h. UEBA

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

e. shadow boxing
f. encryption
g. sandboxing
h. an incident

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

e. Inc
f. Breach
g. Security event
h. FIRE

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

e. Incidents
f. Breaches
g. Events
h. Logs

10. All the following are sandboxing tools except:

e. Talos Intelligence
f. URLVoid
g. Threat Crowd
h. Juniper

Chapter 6 Quiz Answers

Correct answers are marked with an asterisk.

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

e. private
f. public
g. multicloud
h. popular

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

e. private
f. multicloud
g. hybrid
h. public

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

e. secret
f. hybrid
g. compound
h. outcross

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

e. tri-cloud
f. auxiliary-cloud
g. common cloud
h. multicloud

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

e. hypervisor
f. hypovisor
g. inner visor
h. output visor

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

e. of, in
f. in, of
g. before, after
h. between, around

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

e. Software as a Service offers developmental building blocks
f. Platform as a Service is used to deploy binaries and develop data application or stores
g. Desktop as a Service delivers virtual desktop management over the network
h. Infrastructure as a Service is deployment that uses infrastructure components like computing, storage, and network devices.

Chapter 7 Quiz Answers

Correct answers are marked with an asterisk.

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

e. Automation
f. Robots
g. Process
h. Orchestration

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

e. Automation
f. Process
g. Orchestration
h. Inventory

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

e. process, task
f. task, process
g. process, response
h. response, task

4. All the following are true regarding automation except:

e. It will replace analysts in the next five years
f. It streamlines existing processes
g. It frees up analysts from monotonous tasks
h. It manages the flood of events coming in daily

5. All the following are reasons to implement automation except:

e. Reduce analyst fatigue
f. Reduce mistakes
g. Reduce information bias
h. Reduce productivity

6. Which of the following is true regarding how to start automating?

e. Start with complex changes
f. Someone who is intimately familiar with the organization's processes and procedure should analyze the work done each day
g. Categorize the tasks by how much time they take
h. Look for repetitive actions with complex conditions

7. All the following are true about playbooks except:

e. They can be small
f. They can call other playbooks synchronously
g. They're only used in fantasy football
h. They should not cause incorrect or damaging actions

8. In light of automation, why do we still need analysts? All the following apply except:

e. Analysts are needed to detail events
f. Analysts are like robots
g. Analysts are needed to look for trends
h. Analysts are needed to examine data over time

9. All the following are true about orchestration except:

e. It's closely tied to automation
f. It automates more complex workflows
g. It takes advantage of multiple automation tasks
h. It's the opposite of automation

10. All the following are tips for using automation as a security tool except:

e. Write long, complex playbooks
f. Do an inventory of the tasks performed by your SOC
g. Challenge the status quo
h. Focus on simple, quick actions