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 Course 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.