How To Get Started In Cybersecurity

July 6, 2019
by SentinelOne

The cybersecurity skills shortage is a pressing concern for businesses, with the current shortfall estimated to be around 2 million unfilled positions, a number that is expected to rise to around 3.5 million by 2021. If there's an upside to this shortage, it is that for those interested in a career in cybersecurity, there are many opportunities to enter this vast and interesting field.

The question is, though, just how do you get started? While there are many articles about careers in cybersecurity, few answer the practical questions of what you should learn, or give guidance on where you can learn it. In this post, we'll take a look at the entry-level options and offer some practical guidance that addresses just those questions. If you're starting out on your first career or wishing to transition into cybersecurity from other IT-related work such as software development or network administration, then read on.

What Jobs Are There in Cybersecurity?

There are numerous job titles and positions in the field, there's 50 listed here, and many companies will define roles that cross individual disciplines to suit their own needs, but some of the key roles and responsibilities in the field of cybersecurity that are open at an entry-to-intermediate level include the following.

Security Analyst: typically works in a Security Operations Centre or IT team focused on security. An analyst's primary job is incident detection and response. Analysts will be required to triage, investigate, contain and remediate cyber security incidents. They will need to use and operate EDR tools. Their duties will also likely include some threat hunting and incident reporting.

Penetration Tester: may be an independent contractor or in-house staff, the "pen testers" job is to simulate real attacks to find weaknesses in an organization's security. Pen testers go further than just looking for vulnerabilities, though, as their job is not just to show that there is a chink in the armor, but to actively prove that it can be exploited.

Digital Forensics Investigator: the work of those involved in DF/IR (digital forensics/incident response) takes place after a digital crime or breach has been found to have taken place. The cyber crime investigator will typically work with law enforcement officers to identify direct evidence of a crime, collect any evidence that may be used in attribution, and to ascertain as much information as possible about the attackers' actions while on the device through examining digital artifacts.

Malware Researcher: the role of the malware researcher or analyst is to take code written by threat actors and understand what it does, how it does it, and how the organization's security team can detect it. Crucial to the work of a malware researcher is the ability to reverse engineer malware, which involves understanding the internal functions of a program without having access to its source code.

These entry-level to intermediate level positions include several specializations, but there is also a lot of overlap, and most people working in any one of the above roles will have some understanding of the skills required in others. Broadening your skill set will allow you to move up to more senior positions once you have acquired some experience, such as becoming a Senior Threat Analyst, Security Architect or even a CISO (Chief Information Security Officer).

View the infographic

What Skills Are Needed For Cybersecurity?

With such a wide variety of roles and positions, there is an equally large set of KSAs (knowledge, skills and abilities) required to suit various positions, and each field of expertise naturally has its own requirements. However, there are some essential skills that are pretty much appropriate for any job in cybersecurity and the more of these you can tick off, the better your chances of attracting an employer. Among these key skills are your knowledge of operating systems, programming languages and networking. Let's take a closer look at each. All the resources we'll suggest are free unless otherwise stated.

Operating System Essentials

A good understanding of Linux is essential, as it's widely used to run web servers and other business computers, powers Android and IoT devices and also makes a great Desktop platform for many cybersecurity tasks. Linux has an abundance of freely accessible tools for security analysts, penetration testers and malware analysts. A Linux box can serve as a workhorse to help you develop key skills that will transfer across many different cybersecurity roles and positions. The key to mastering the Linux operating system lies primarily in mastery of the command line, so once you have a Linux OS up and running, that's where you should head.

Learning Resource: Intro to Linux (LFS101)
Learning Resource: Linux Command.org

Of course, you should know your way around Windows, as it is still by far and away the most prevalent Desktop OS in and out of the enterprise, and consequently faces the most attention from cybercriminals. Go beyond the user basics and start learning how to use tools like Procmon, the Registry Editor, Task Manager and the Sysinternals Suite.

Learning Resource: Microsoft Sysinternals Suite

If you're interested in macOS, which is becoming more common in the enterprise, you'll need a Mac computer as the OS doesn't (technically or legally) run on non-Apple hardware. Learning about Macs from a security angle isn't quite as easy as with other operating systems as there are fewer resources. Apple do provide some training courses, but they are not free and focus more on support and administration. If you have a good understanding of Linux, however, this will stand you in good stead as the Mac is built on a Unix platform.

Learning Resource: How Malware Persists on macOS
Learning Resource: Malware Hunting on macOS | A Practical Guide

Programming Skills

In almost every job in cybersecurity you'll be expected to use some programming languages and to be able to understand programming concepts. Aside from learning how to use shell scripts (see our learning resource for Linux above), you should have some familiarity with the following.

Python is the most widely used admin and cybersecurity tool on all OS platforms, and pretty much any job will require you to have at least a working knowledge of the language. Ideally, you should have a bit more than that, and it's a safe bet that if you do most of your day-to-day coding with Python you'll be able to handle the programming tasks in the majority of cybersecurity positions.

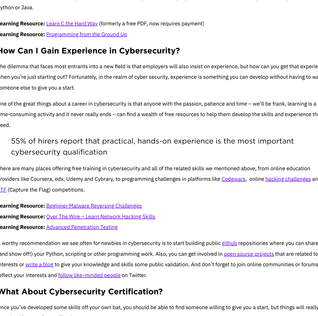
Learning Resource: LearnPython.org

As the majority of cyber attacks leverage web technologies somewhere in the kill chain, whether it's a poisoned website or C2 server to control a botnet, JavaScript is something you should be comfortable with at least reading, if not writing.

Learning Resource: Coursera Learn Javascript (free, but requires payment for certification)

If you're focused on positions involving Windows malware or threats created in any of Microsoft's programming languages like VBA, PowerShell or C#, then knowledge of .NET APIs and Windows programming with C++ will be a great way to make you stand out as a candidate.

Learning Resource: Microsoft C# Tutorials
Learning Resource: Microsoft Professional Program for Cybersecurity (free, but requires payment for certification)



If you are interested in bug hunting and bug bounty programs, malware analysis and reverse engineering across platforms, one of the most essential skills to develop is programming in C and Assembly language. While few people would recommend learning C these days for general programming positions – the language has so many security issues, it's almost frowned upon – the fact is that most of the code you'll deal with in cybersecurity is C under the hood, and if you can code in C, being able to read and understand higher level languages is an easy translation. An understanding of C will also make learning assembly language a far easier jump than it might be coming from, say, Python or Java.

Learning Resource: Learn C the Hard Way (formerly a free PDF, now requires payment)
Learning Resource: Programming from the Ground Up

How Can I Gain Experience in Cybersecurity?

The dilemma that faces most entrants into a new field is that employers will also insist on experience, but how can you get that experience when you're just starting out? Fortunately, in the realm of cyber security, experience is something you can develop without having to wait for someone else to give you a start.

One of the great things about a career in cybersecurity is that anyone with the passion, patience and time – we'll be frank, learning is a time-consuming activity and it never really ends – can find a wealth of free resources to help them develop the skills and experience they need.

> 55% of hirers report that practical, hands-on experience is the most important cybersecurity qualification

There are many places offering free training in cybersecurity and all of the related skills we mentioned above, from online education providers like Coursera, edx, Udemy and Cybrary, to programming challenges in platforms like Codewars, online hacking challenges and CTF (Capture the Flag) competitions.

Learning Resource: Beginner Malware Reversing Challenges
Learning Resource: Over The Wire – Learn Network Hacking Skills
Learning Resource: Advanced Penetration Testing

A worthy recommendation we see often for newbies in cybersecurity is to start building public github repositories where you can share (and show off!) your Python, scripting or other programming work. Also, you can get involved in open source projects that are related to your interests or write a blog to give your knowledge and skills some public validation. And don't forget to join online communities or forums that reflect your interests and follow like-minded people on Twitter.

What About Cybersecurity Certification?

Once you've developed some skills off your own bat, you should be able to find someone willing to give you a start, but things will really speed up if you go for certification.

None of the resources here are free, and you should already be confident in your current skills and your ability to learn at pace before considering them. That said, these kind of certifications will add validation to the skills and experience you have developed and are a good way to convince an employer that you're up to the task.

One of the most well-respected names in penetration testing and ethical hacking is Offensive Security, the people behind the Kali Linux operating system. They offer a number of paid courses that have a reputation for being both tough and applicable to the real world.

Learning Resource: Penetration Testing Training with Kali Linux (OSCP)

CompTIA certification has probably been around longer than most, and their Security+ exam ensures potential employers that you have a strong foundation in security threats, vulnerabilities, technologies and tools, secure network architecture and more.

Learning Resource: CompTIA Certifications

When it comes to validating security chops, probably the biggest name around is the SANS Institute. They offer a huge variety of courses for just about every role imaginable. They also may be beyond your means, however, unless you already have an employer willing to fund your training.

Learning Resource: Hacker Tools, Techniques, Exploits and Incident Handling (SEC504)

Just be aware that certification doesn't really trump experience at the entry level, and not all certifications carry real-world practical use, so be sure to check out that any course you're going to pay for is both from a recognized trainer like those mentioned above and is teaching up-to-date, relevant skills.

Do I Need A University Degree to Work in Cybersecurity?

While most intermediate and senior level jobs in this field will require you to have some kind of bachelors or higher degree, many people start out with nothing more than a keyboard and an interest in "breaking things" – the hacker mentality. However, many more doors will swing open if you have a bachelors or Masters degree in a cybersecurity-related discipline.

Of course, any degree worth its salt will require some kind of funding, but if you're already on the education treadmill and have the opportunity to choose a related degree or Master degree path, there are a multitude of options depending on your location.

Learning Resource: Use a getsecedu to find local or online courses in cybersecurity

If you are interested in studying for a Master's degree online, edx offer a program from Georgia Tech.

Learning Resource: Master's Degree in Cybersecurity

Conclusion

Threat actors have been getting more numerous and more dangerous in recent years and that's a trend that is only likely to continue. The need for businesses to hire skilled staff to combat the threat provides plenty of opportunities for anyone with the tenacity and talent to get involved in cybersecurity. With a wide choice of possible roles, and plenty of available learning resources as we've covered in this post, this is an ideal time to pursue a career that will be challenging, rewarding and a valuable service to the community.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- 11 Bad Habits That Destroy Your Cybersecurity Efforts
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- Fortune Names SentinelOne a Top Workplace in Tech
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls
- Advancing Security | The Age of AI & Machine Learning in Cybersecurity