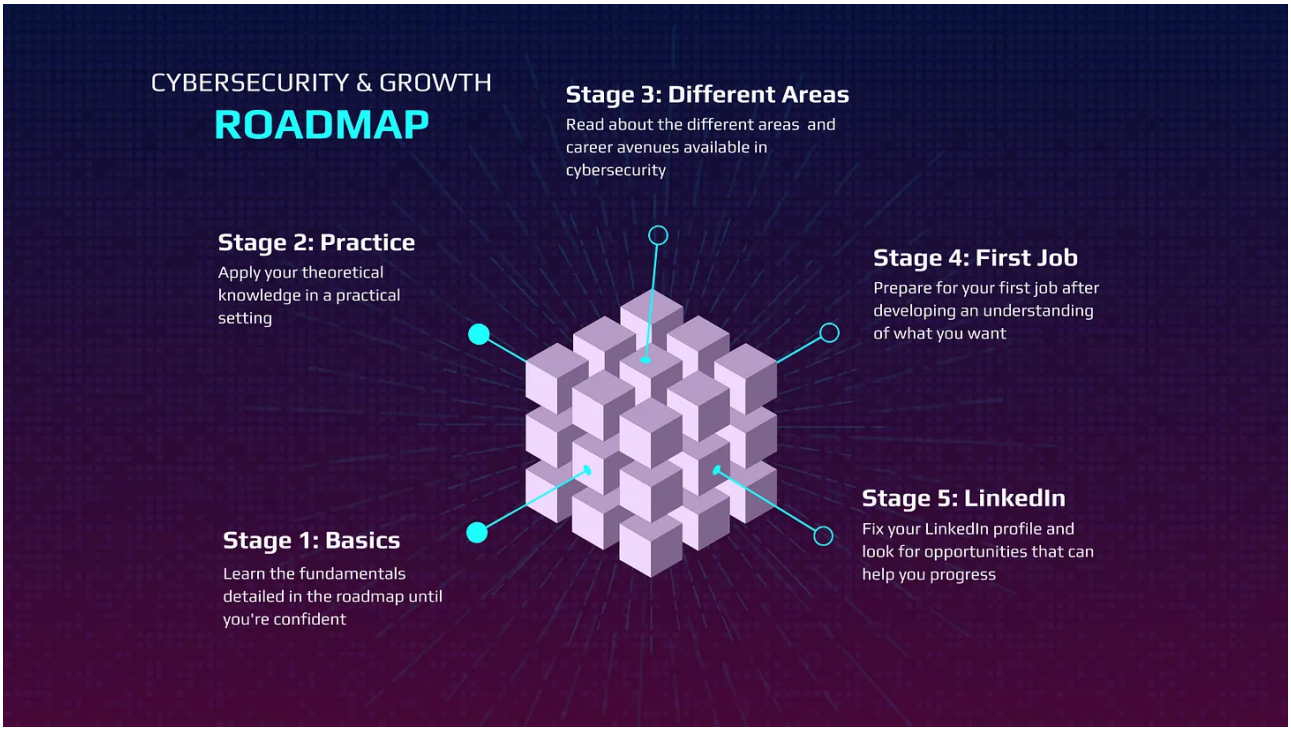
A Roadmap To Your First Cybersecurity Job

Follow this roadmap if you want to learn more about cybersecurity and are unsure where to start. It covers what you need to do and how to do it.

DANIEL KELLEY

25 MAR 2023



Here's A Quick Opening Note

Before we get started, I highly recommend purchasing a membership plan upgrade so that you can join our private community. In this community, you'll be able to network with other like-minded individuals that are interested in progressing. There's almost always someone available to answer any questions you may have. Additionally, you'll gain access to an exclusive archive of content that's published through thisnewsletter.

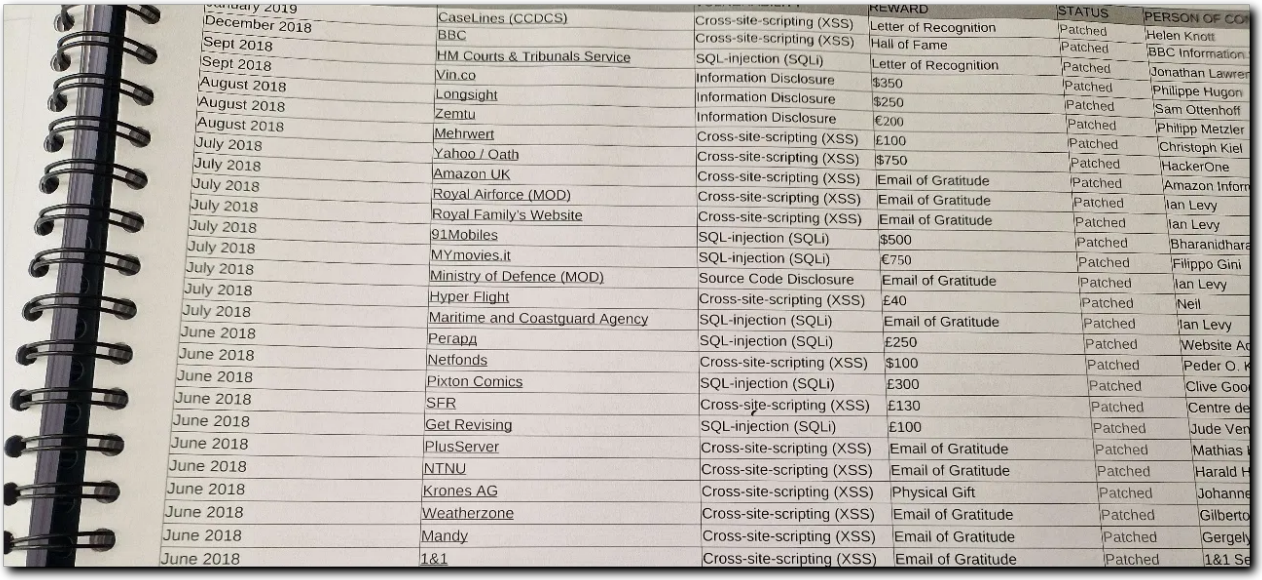
The Success Of This Roadmap

The success of this cybersecurity roadmap is ultimately contingent upon the dedication and effort you invest in mastering its components. While this roadmap equips you with the essential tools, knowledge, and resources to learn, it is crucial to remember that your personal growth and expertise in cybersecurity is directly proportional to your commitment and determination. The roadmap serves as a comprehensive guide, but the onus is on you to actively engage with the material, ask questions, and apply what you've learned to real-world situations. Your journey in cybersecurity requires consistent hard work, persistence, and an innate curiosity to delve deeper into it.

My Personal Beginning

When I first started learning information security (now known as cybersecurity) in 2012, things were different. As a young teenager, I began by browsing technology forums to learn various concepts. I'd spend one week exploring operating systems, another on programming, and another on web-application development, resulting in a scattered foundation. Back then, I had no real intent to transition into the industry itself; it was more of a curiosity because I found these topics fascinating.

After immersing myself in these forums for a year or two, I unearthed a passion for web application security and devoted myself to it for nearly five years. As a result of my dedication, I made significant contributions to over 100 bug bounty programs.



			REWARD	STATUS	PERSON OF CO
December 2018	CaseLines (CCDCS)	Cross-site-scripting (XSS)	Letter of Recognition	Patched	Helen Knott
Sept 2018	BBC	Cross-site-scripting (XSS)	Hall of Fame	Patched	BBC Information
Sept 2018	HM Courts & Tribunals Service	SQL-injection (SQLi)	Letter of Recognition	Patched	Jonathan Lawren
August 2018	Vin.co	Information Disclosure	$350	Patched	Philippe Hugon
August 2018	Longsight	Information Disclosure	$250	Patched	Sam Ottenhoff
August 2018	Zemtu	Information Disclosure	€200	Patched	Philipp Metzler
July 2018	Mehrwert	Cross-site-scripting (XSS)	£100	Patched	Christoph Kiel
July 2018	Yahoo / Oath	Cross-site-scripting (XSS)	$750	Patched	HackerOne
July 2018	Amazon UK	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Amazon Inform
July 2018	Royal Airforce (MOD)	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Ian Levy
July 2018	Royal Family's Website	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Ian Levy
July 2018	91Mobiles	SQL-injection (SQLi)	$500	Patched	Bharanidhara
July 2018	MYmovies.it	SQL-injection (SQLi)	€750	Patched	Filippo Gini
July 2018	Ministry of Defence (MOD)	Source Code Disclosure	Email of Gratitude	Patched	Ian Levy
July 2018	Hyper Flight	Cross-site-scripting (XSS)	£40	Patched	Neil
July 2018	Maritime and Coastguard Agency	SQL-injection (SQLi)	Email of Gratitude	Patched	Ian Levy
June 2018	Перард	SQL-injection (SQLi)	£250	Patched	Website Ac
June 2018	Netfonds	Cross-site-scripting (XSS)	$100	Patched	Peder O. K
June 2018	Pixton Comics	SQL-injection (SQLi)	£300	Patched	Clive Goo
June 2018	SFR	Cross-site-scripting (XSS)	£130	Patched	Centre de
June 2018	Get Revising	SQL-injection (SQLi)	£100	Patched	Jude Ven
June 2018	PlusServer	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Mathias
June 2018	NTNU	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Harald H
June 2018	Krones AG	Cross-site-scripting (XSS)	Physical Gift	Patched	Johanne
June 2018	Weatherzone	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Gilberto
June 2018	Mandy	Cross-site-scripting (XSS)	Email of Gratitude	Patched	Gergely
June 2018	1&1	Cross-site-scripting (XSS)	Email of Gratitude	Patched	1&1 Se

Reflecting on my earlier years as a generalist, I see both a downside and an upside. The downside was that I never became particularly skilled in any one area, while the upside was that I had some form of knowledge about everything. When people ask me how I learned, I can't rely on my personal experiences to help them, because much of my practical knowledge came from illicit computer hacking and simply playing around with technology, dedicating hundreds of hours to it as a young teenager. I did most things because I enjoyed them, not because I wanted to transition into information security or cybersecurity.

I've designed this roadmap to incorporate properties that I believe would be helpful for someone transitioning into cybersecurity, based on my experience. This approach is highly goal-oriented. It will teach you the fundamentals, and then you'll arrive at a crossroads where you'll need to explore various aspects of cybersecurity and choose a specific path to pursue. The roadmap cannot cover every single possibility, as it would then become a book, and there are certain areas I wouldn't feel comfortable advising on due to my limited experience with them.

After you decide what it is that you want to do and what you're interested in, you should seek out the appropriate resources to take you deeper into that avenue. If you want to explore a SOC career, you should seek out SOC resources; if you want to explore being in incident response, you should seek out incident response resources, etc.

Covering The Fundamentals

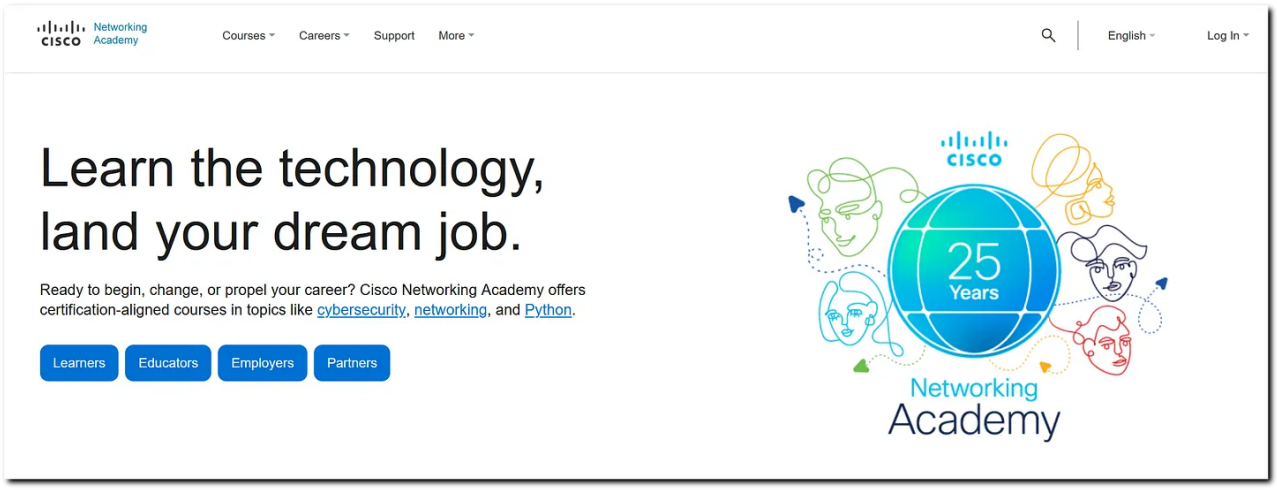
In this roadmap, I won't be covering aspects like physical equipment. Any device will do; you don't need an expensive MacBook to learn cybersecurity, nor is a specific type of computer necessary. I've heard of people learning and contributing to bug bounty programs using mobile devices and tablets (hard to believe, but genuinely true). So, before we begin, here are the fundamental categories that I believe can be applied across any avenue you choose to pursue in cybersecurity:

Hardware Properties

At the very least, you need to be familiar with the basic components inside your laptop or computer. Not only is this beneficial for your overall knowledge, but it also provides an ideal and simple starting point. I gained familiarity by disassembling an old computer and reassembling it. Over the years, I have also troubleshooted various issues.

- **freeCodeCamp Computer Basics** - Watch all 43 videos. They're short and informative.
- **PowerCert Animated Videos** - Good for picking up the different concepts.
- **The Hidden Language of Computer Hardware and Software** - Fun read. It's pretty high level in terms of abstraction but one of my favourites.

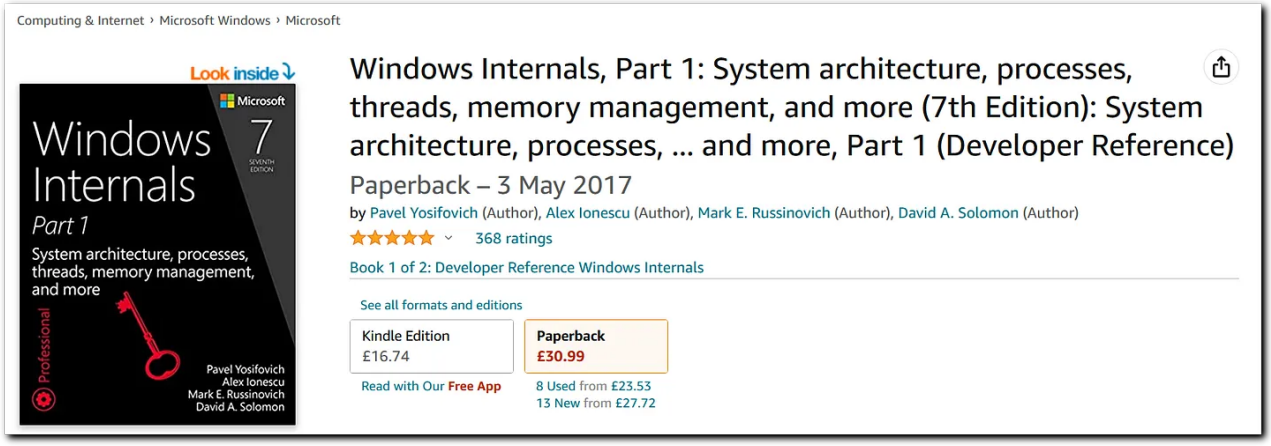
Networking Concepts



Networking is quite essential, but you don't have to be some guru with it to progress in cybersecurity. Many people will tell you that you need to understand a great deal about networking, but I've found this to be somewhat exaggerated. Grasping the basics, like protocols, understanding the different types of networks, network security, and basic security hygiene, is more than sufficient.

- **Cisco Networking Academy** - I've explored various resources on networking devices over time. Cisco Networking Academy provides comprehensive material and practical exercises.
- **Computer Networking: A Top-Down Approach** - This book offers a solid foundation on network protocols and explains the concepts in an easy-to-understand manner.

Operating Systems



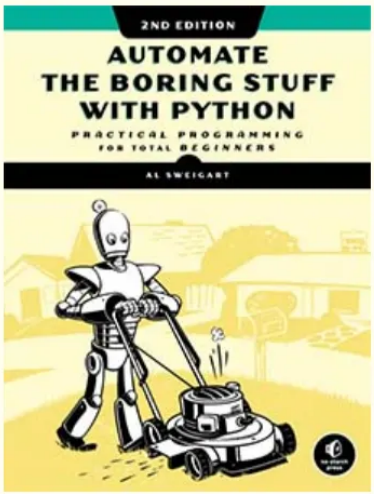
My advice here would be to choose an operating system to begin with, and then learn as much as you can about it. Ideally, you should aim to learn a few things about the command line interface (CLI). For Windows, this would be PowerShell, and for Linux, Bash. It sounds a lot more complicated than it really is. Of course, a brief understanding of their security mechanisms and how they work in general is ideal.

- **Linux Inside: 0xax** - This is an underrated resource. It will help you familiarize yourself with Linux and its different aspects on a deeper technical level.
- **Windows Internals** - The authors thoroughly explain key concepts, including memory management, system mechanisms, and the intricacies of various subsystems.
- **Operating Systems: Three Easy Pieces** - This is a good book for learning operating system concepts overall. It's available for free online, and covers topics like virtualization, concurrency, and persistence.

Programming Fundamentals

AUTOMATE THE BORING STUFF WITH PYTHON

By Al Sweigart. Over 500,000 copies sold. Free to read under a CC license.

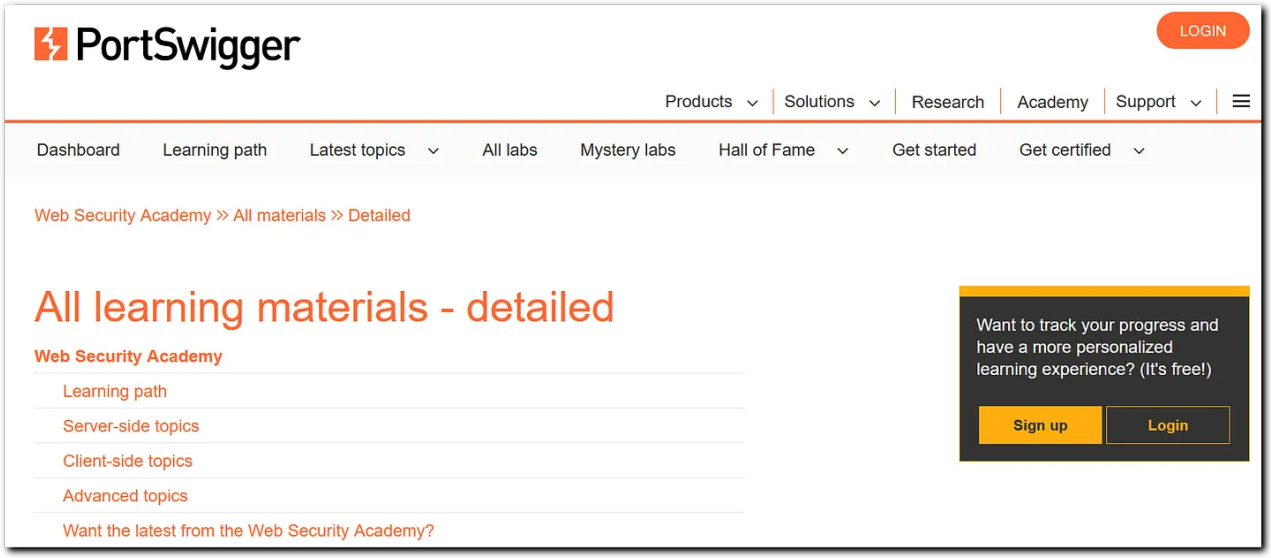


"The best part of programming is the triumph of seeing the machine do something useful. Automate the Boring Stuff with Python frames all of programming as these small triumphs; it makes the boring fun."
- Hilary Mason, Data Scientist and Founder of Fast Forward Labs

The challenge with programming is that there are countless resources available, and what works for me may not always work for you. For popular topics like this, I encourage you to conduct your own research and discover valuable resources. Aim to learn the fundamental concepts of programming, such as loops, variables, and arrays etc, and at the very least, familiarize yourself with a scripting language like Bash or Python.

- **thenewboston YouTube Channel** - I've watched hundreds of videos on programming over the years. He explains things in a clear and concise manner.
- **Automate the Boring Stuff with Python** - This is good for learning Python overall.
- **Harvard CS50 Web Programming** - A really good introduction to the fundamentals.

Web-Application Security



When referring to web application security, the basics can provide sufficient coverage depending on your objectives. Understanding concepts such as HTTP and familiarizing yourself with common web application vulnerabilities will be highly beneficial.

- **The Web Application Hacker's Handbook** - First book I ever read that taught me a bunch of concepts, I still refer to it even to this day.

- **The OWASP Top 10 Project** - Industry standard when it comes to looking at web-application security.
- **PortSwigger Web Security Academy** - This is good for learning common web-application vulnerability types.

Exploring The Fundamentals

These fundamentals should be sufficient to bring you to a point where you can decide to delve further into a specific avenue. Learning can be accomplished in various ways, such as watching videos, reading blog posts, reading books, completing challenges, or diving right in. The resources provided are valuable, and I would personally use them. Of course, there are a million other ways to learn, and I encourage you to explore other materials that cover these categories.

The best way to discover information is to search for specific points related to the categories above. For example, if I'm looking at SQL injection vulnerabilities, I would specifically input that into Google and try to learn as much as I can about SQL injection. I don't recommend relying on just one resource to learn everything. This is where you need to venture out on your own and do some research. I can only provide examples of what good material looks like.

In the beginning, your approach will likely be more theoretical, but I firmly believe that the most effective way to learn is through practical experience. Therefore, you should aim to engage in hands-on activities as much as possible.

Putting Theory Into Practice

After mastering the fundamentals, your next step is to find a way to apply the skills you've learned in a practical manner.

Build A Home Lab

- **Resource:** "Homelabbity" (https://www.reddit.com/r/homelab/wiki/index/)
- **Benefits:** A home lab allows you to experiment with different technologies, test your skills in a safe environment, and gain hands-on experience with real-world scenarios.

- **Opinion:** Building a home lab can be a highly rewarding experience, as it not only provides you with a sandbox to experiment and learn but also demonstrates your commitment to mastering the subject matter. However, it might require a significant investment of time and resources.

Produce Blog Posts

- **Resource:** Medium (**https://medium.com/**)
- **Benefits:** Writing blog posts helps you solidify your understanding of a topic, improve your communication skills, and build an online portfolio that showcases your expertise.
- **Opinion:** Producing blog posts is an excellent way to engage with the community, share your knowledge, and give back. Plus, it helps you establish a personal brand and network with like-minded professionals.

Practice On Online Training Platforms

- **Resource:** HackerRank (**https://www.hackerrank.com**) for programming challenges, TryHackMe (**https://tryhackme.com/hacktivities**), and Hack The Box (**https://www.hackthebox.eu/**) for cybersecurity exercises.
- **Benefits:** Online training platforms offer a wide range of challenges and exercises to improve your skills, learn from others, and track your progress over time.
- **Opinion:** Online training platforms are an invaluable resource for honing your skills and staying up to date with the latest trends and techniques. They provide a structured and engaging learning environment, making them an excellent choice for anyone looking to level up.

Write Your Own Tools Or Scripts

- **Resource:** GitHub (**https://github.com**) to host and share your projects
- **Benefits:** Writing your own tools or scripts helps you develop problem-solving skills, gain a deeper understanding of the technologies you're working with, and create custom solutions tailored to your needs.
- **Opinion:** Developing your own tools or scripts can be a game-changer, as it demonstrates your ability to innovate and think critically. Automation is also a

massive aspect of cybersecurity.

Personal Opinion And Advice

Personally, I would focus on producing blog posts and practicing on online training platforms like HackerRank, TryHackMe, and Hack The Box. These options provide a balance between sharing your knowledge, improving your skills, and staying engaged with the community.

The overall idea is to prove to yourself that you've actually absorbed the information and can apply it in practical scenarios, so you're not just filled with theoretical knowledge. By engaging in hands-on activities and sharing your experiences through blog posts, you reinforce your learning and demonstrate your competence to potential employers.

Exploring The Different Areas Of Cybersecurity

So by now, you should at least have a solid comprehension of the fundamentals and have chosen a way to engage in practical activities to demonstrate the theory you've learned.

The next step is to deliberately explore the different areas of cybersecurity. I recommend doing this by looking at the **UK Cyber Security Council's Cyber Career Framework**. It's the most comprehensive roadmap I've come across and is not filled with fluff or countless options. Now, while reviewing this roadmap, you should fill out the spreadsheet below with job titles from it.

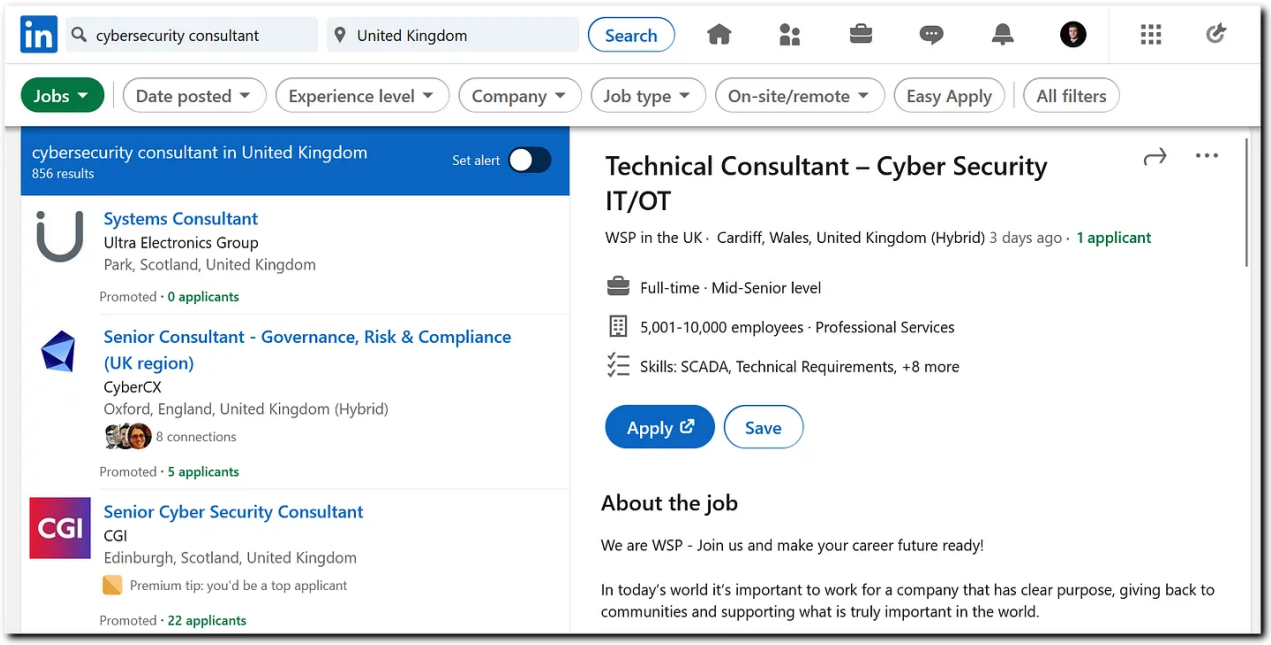
Download The Spreadsheet

It may seem odd, but bear with me. You'll see where I'm going with this in a moment. After filling out the spreadsheet, it should look like this:

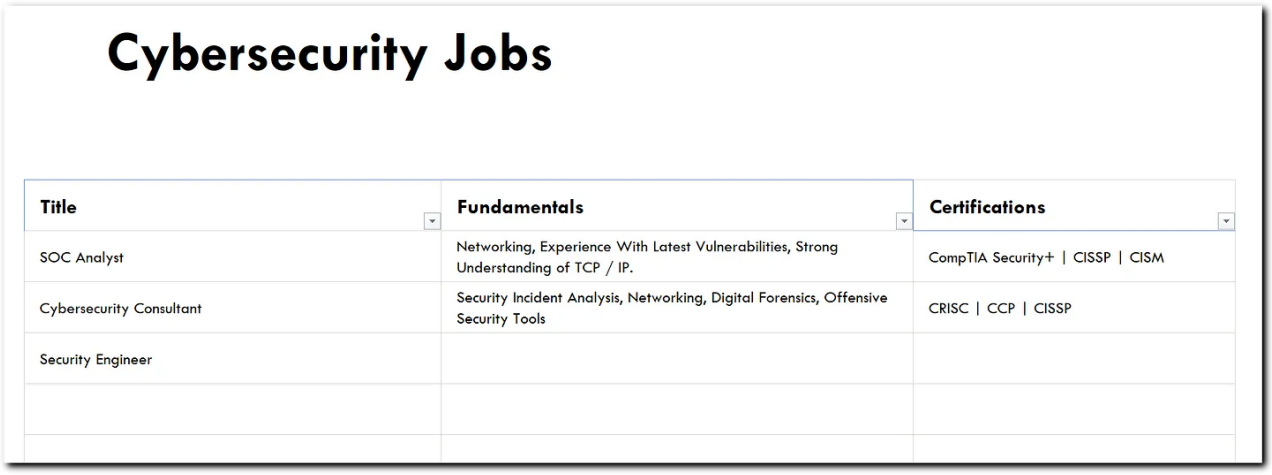
Cybersecurity Jobs

Title	Fundamentals	Certifications
SOC Analyst		
Cybersecurity Consultant		
Security Engineer		

Next, head to LinkedIn and paste all the job titles you've collected into the search bar. After some searching, if you pay close attention, you'll notice that similar positions have similar job requirements.



Now start to fill in the rest of the spreadsheet with the common requirements, and the certifications required, specifically.



Cybersecurity Jobs

Title	Fundamentals	Certifications
SOC Analyst	Networking, Experience With Latest Vulnerabilities, Strong Understanding of TCP / IP.	CompTIA Security+ | CISSP | CISM
Cybersecurity Consultant	Security Incident Analysis, Networking, Digital Forensics, Offensive Security Tools	CRISC | CCP | CISSP
Security Engineer		

Once you have identified the common requirements and certifications, begin working towards obtaining them. If you find that you are struggling to pass the certifications, consider revisiting the fundamentals or seeking more specific resources related to the certification you are pursuing.

I will not go through every single certification out there, nor the appropriate resources for each one, but as an initial recommendation, I suggest considering any of the **CompTIA certifications**, specifically Security+. It is an excellent starting point, and I have seen people land jobs in the industry with just this certification. It is more suitable for those trying to enter the industry.

For anything CompTIA-related, I highly recommend checking out Professor Messer's YouTube Channel.

View The YouTube Channel

It's one of the most comprehensive study resources I've seen for anything CompTIA related. **CompTIA is a path that I recommend you go down**.

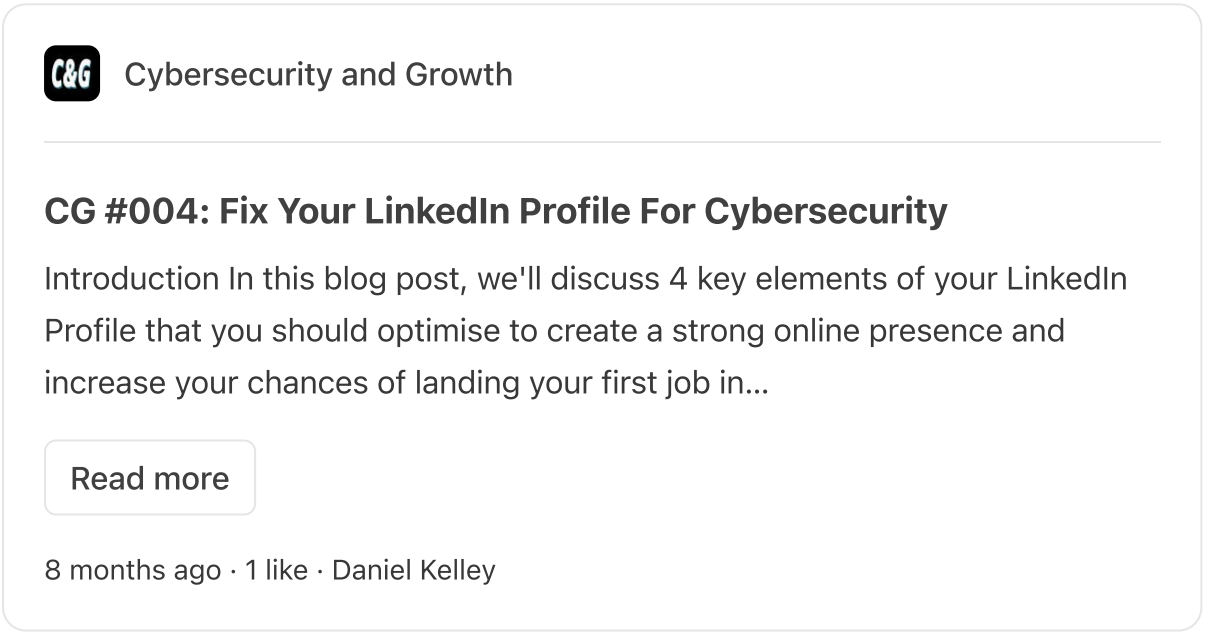
Looking For Your First Job

By now, you should have learned the fundamentals, participated in one or more practical activities to showcase your competence, and ideally obtained at least one certification (or be in the process of earning it). At this stage, I believe you're well-prepared to start searching for your first entry-level position in the industry. There are numerous websites available for this purpose.

However, for the sake of this road-map, I'm going to be focusing on LinkedIn because it's the biggest network out there when it comes to connecting with potential employers.

Fixing Your LinkedIn Profile

If you don't have an account on LinkedIn, I highly recommend creating one. Opportunities are posted there all the time, and it's possible to connect with peers and employers. The next step is to tidy up your LinkedIn profile. Unfortunately, I know quite a bit about this because I spend far too much time on the website. So, here's how I would go about tackling that:



I'm not going to teach you how to use LinkedIn unless there's a demand for it, but basically, the only rule I'd follow is to avoid posting negative content. Many people do it, and I don't understand why; it's unwise because people, including future bosses, can form opinions quite quickly based on what they see.

Final Words On This Roadmap

And that's essentially it. All of this should be enough to at least secure you an entry-level role in cybersecurity. Yes, the job market can be competitive, and yes, it requires consistency, but from experience, most people in entry-level roles are at this level. **So by now, you should have the following:**

- An understanding of the fundamentals.
- A certification or two.
- Practical examples of what you've done.
- A solid LinkedIn profile.

As a final point of call, I also suggest staying up-to-date with the areas of cybersecurity that interest you.

Please note that this is my personal roadmap, based on the advice I've provided to others. I know at least 3 individuals who have followed this guidance, despite coming from non-technical backgrounds, and successfully secured jobs in cybersecurity. Some seasoned professionals in the industry may scoff at the idea of using LinkedIn or following a roadmap at all. However, it is important to acknowledge that the hiring process has evolved significantly over time.

Previously, cybersecurity was not considered an entry-level field. Typically, one would begin their career in information security (IT), perhaps as a network engineer, and then transition to a security role or department. It's crucial to recognise that those who exhibit a dismissive attitude might be more focused on gatekeeping than providing genuine guidance.

That said, this is not the only roadmap out there. **Here are another 2 roadmaps that you can look at and explore:**

- **How to Build a Cybersecurity Career**
- **Create Your Cybersecurity Roadmap**

But if you take a closer look, you'll see they all have one thing in common: learning and practicing the basics in different ways. How you choose to do that is up to you, but in the end, that's what it's really all about when trying to break into the field.

2 Comments

Write a comment...

Pawel Burdzy Apr 1 ♥ **Liked by Daniel Kelley**

Fundamentals, you said... A lot of to cover but there's no other way it seems. Thank you.

LIKE (1) REPLY SHARE

1 reply by Daniel Kelley

1 more comment...