How to successfully break into Cyber security?

You are a successful experienced IT professional (non-cyber) or a beginner who wants to enter Cybersecurity field. How can you do? What things to be considered? Are there any best approach or steps for this process? In this guide I am going to share an approach you can follow to successfully break into cybersecurity.

Email: chintangurjar@outlook.com
LinkedIn: https://www.linkedin.com/in/chintangurjar/

Table of contents

23. As a beginner what all challenges I can face? OR What are some of the challenges faced by beginner?
24. How can I stay up-to-date with latest knowledge in cybersecurity or a specific domain within cyber?
25. Why cannot I become a CEO straightout of my master's degree? Don't become CEO because you are good at just talking or teaching.
26. How can I not get demotivated? OR What to do when I get demotivated?
27. I work in XYZ field of IT, how can I jump into cybersecurity domain from there?

Three main components of entering into the Cybersecurity domain

1. Understand the scale of the spectrum
2. Create & meet your requirements/ needs
3. Plan & execute it

8 Steps of the Approach

Keep doing your current job (If you are not doing a job, skip to the next part)
It is vital to keep earning with your current job until and unless you have successfully entered the Cybersecurity field with a full-time job. Your family might be dependent on you.
Do not take a break for specific study/course/certifications/masters if you already work in the non-cyber-IT field.

How to know what all domains there are in cybersecurity in the first place?
Refer to CISO mind map. **https://www.sans.org/posters/ciso-mind-map-and-vulnerability-management-maturity-model/** **https://rafeeqrehman.com/2023/03/25/ciso-mindmap-2023-what-do-infosec-professionals-really-do/**
Understand how many various domains there are in the security field.
Take each bullet point from that PDF and Google or ChatGPT it. Ask the below questions yourself:
1. What is that domain?
2. What kinds of roles/titles/designations does the company offer in that domain?
3. What free/open-source/commercial tools and solutions do people/companies use?
4. What are day to day routines/roles and responsibilities do people have in that job role?
5. Is it demanding or not? What could be the potential future?

6.	Which reputable organizations provide certifications in that domain?
7.	Look for the course syllabus of that cert to understand what can be covered?
8.	Does that fancy you?
9.	Which roles can you start within that domain as a beginner, and where can you reach a maximum in terms of designation?
10.	What will be the future of that domain?
11.	What are the technical prerequisites required to land a successful first job in this domain?

CH

I am a beginner in the cybersecurity domain. Before I start my career, I want to know the various fields into cybersecurity. I have already found a list of various cyberdomains and I have picked 3 domains. For now I want to know the below things about these 3 cyber domains so I can make better decision whether should I start with these domains or not.

The first one is Threat Intelligence.

1. What is that domain?
2. What kinds of roles/titles/designations does the company offer in that domain?
3. What free/open-source/commercial tools and solutions do people/companies use?
4. What are day to day routines/roles and responsibilities do people have in that job role?
5. Is it demanding or not? What could be the potential future?
6. Which reputable organisations provide certifications in that domain?
7. Which roles can you start within that domain as a beginner, and where can you reach a maximum in terms of designation?
8. What are the technical prerequisites required to land a successful first job in this domain?

Sure, let's start with Threat Intelligence:

What is that domain?

Threat Intelligence is a domain of cybersecurity that involves the collection, analysis, and dissemination of information about potential or current attacks that threaten an organization. It focuses on understanding the tactics, techniques, and procedures (TTPs) used by threat actors, determining their objectives, and predicting their future activities.

What kinds of roles/titles/designations does the company offer in that domain?

There are various roles within the Threat Intelligence field. Some of them are Threat Intelligence Analyst, Threat Intelligence Engineer, Threat Intelligence Specialist, Threat Hunter, Threat Intelligence Manager, and Director of Threat Intelligence.

What free/open-source/commercial tools and solutions do people/companies use?

Threat intelligence platforms (TIPs) are commonly used in this domain. Some well-known commercial TIPs include Recorded Future, ThreatConnect, and Anomali. Open-source intelligence (OSINT) tools, such as Maltego and TheHive, and threat intelligence feeds (like AlienVault OTX) are also used.

Refer IT to Cyber domain mapping (This is for the people who work in IT and want to start into Cybersecurity)
Refer to the IT to Cyber mapping table. ***(Appendix 1)***
Understand your position in which and the IT field you are currently working in.
Understand what possible options/areas you can start your journey with within cybersecurity.
If you are an absolute beginner with no IT experience, you can select any field you are interested in. Maybe you would choose domains close to your IT role or possibly completely separate as you are willing to learn new things from scratch. Any approach would work here.

Study Option	Why	Pros	Cons	Resources/How-to
Read a book	Books on any domain can provide comprehensive knowledge on the subject from beginning to end.	Detailed, structured, can learn at your own pace starting from scratch to advance level. Deep, comprehensive knowledge. Encourages independent thought.	- Time consuming - Can be theoretical, might not offer practical experience. - Some books are Paid - Free books are always often too old - Requires motivation and self-discipline.	Libraries, bookstores, eBooks. Plan by setting reading goals. 1. Go to Amazon or other book stores 2. Seach your interested domain in Amazon. 3. Filter the result by 'Publication date'. 4. Order book. 5. Read. **Review:** - Author history - Starts of the book - Table of contents
YouTube Playlist	Watching a series of videos on YouTube about a specific topic.	- Easy way to grasp topic. - Free & easy access. - Flexible. Wide variety of content.	- Depending upon channel creators' views and opinions, the study approach can vary. - No. of topic coverage & in-depth content may also vary. So, you will require to do a lot of research before selecting any particular course on YouTube as they are free.	YouTube, educational channels. Structure by finding a reputable source and following their content. 1. Search for a topic on YouTube. 2. Use YouTube's filter section. 3. Select 2 filters. 1) Type – Playlist 2) Sort by – Upload Date. This will provide you the entire playlist on that topic but sorted by latest uploaded on the YouTube.
ChatGPT	Interacting with AI models like ChatGPT to learn.	Accessible. Interactive learning.	- Limited to text-based interaction. Some information may be outdated. - Also it depends whether you know how to ask specific and relevant questions.	OpenAI's ChatGPT platform. Engage in Q&A sessions.

			- You may need to learn prompt engineering first to take out maximum from ChatGPT	
Official Certification	Some people feel that they can't feel motivated if they don't have any goals/challenges. Hence, they go for paid certifications as once they spend money, they will require to study and crack the exam in a limited timeframe. This keeps them motivated and focused on achieving the goal. Some reputed certification authorities are ISC2, eLearnSecurity, SANS/GIAC, Offensive Security, CompTIA, ISACA, and Mile2.	- Demanded in job descriptions. - Later or sooner you will have to go for that. - Provides proof of knowledge. Recognized by employers.	- Limited time to complete lab/cert - Expiration dates for some certs. - Paid (can be expensive)	Refer to the **Which certifications should I go for?** Section in order to decide which certification you should go for. Here is the **list** of every single Cybersecurity certification available on ther Internet categorized by cert authorities.
Online Course (Pluralsight/Udemy/Coursera/Oreilly	These are some popular portals for studying the entire course of any security domain. Trainers on these platforms are well experienced, and these portal owners also review course content. Ensure you check the ratings of the course before you select and start.	- Courses you may not find on YouTube directly, can be found on these training portals. - Structured learning. Variety of topics. - Various authors for same topic so you can choose which delivery method you may like	- Some courses are overrated - Some authors are overrated. - Quality content might be paid. - Quality may vary	Login and search for the free course. Enroll and learn. **Review:** - Author and course rating but do your own research
Freeform well-structured self-study via Google & YouTube	Manier times, you cannot or don't want to spend money on material as it can be found via Google. So, you can follow this approach. Before starting self-study, all you need to do is select a particular field. Find a famous book on Amazon with good ratings and is not older than a maximum of 6 years. Find a table of contents of that book. E.g., You found a book on Amazon.com. Refer to its table of contents what all they will teach in that book. Then Google each topic, read, and study. Watch practical/theory explanation videos from YouTube. Prepare your notes.	You can become more proactive in terms of grasping different knowledge but filtering the best information to your brain.	- Can be time consuming - Will be hard to different author's knowledge when you search them on various portals each week.	Explained in the Why section.
Self-Learning Projects	Embarking on a personal project related to the field of interest.	Practical application. Personalized learning.	- No guidance. - Success depends on self-motivation.	Personal interest. Create a project plan and follow through.
Podcasts	Listening to podcasts about a specific subject.	- Convenient learning while multitasking (You can listen it while travelling or doing some other work).	- Passive learning. Depth of knowledge may vary. - Follow up practice and practical is required	Podcast platforms like Spotify, Apple Podcasts. Choose a series and follow episodes. There are specific Cybersecurity podcasts

		- Saves time due to multi tasking		such as 'Darknet Diaries' which provides tremendous amount of knowledge.
MOOCs	Massive Open Online Courses offering structured learning on various topics.	Access to course material from top universities. Some are free.	Not all provide certification. Quality varies.	edX, Coursera, FutureLearn. Follow the course syllabus.
Peer Learning Groups	Joining or forming a group to learn together.	Collaborative learning. Immediate feedback.	Scheduling conflicts. Group dynamics may vary.	Meetup, student groups. Schedule regular meetings and follow a study plan.
Tutoring/Coaching	Hiring a tutor or coach for personalized guidance.	Tailored learning plan. Individual attention.	Can be expensive. Quality depends on the tutor.	Tutoring platforms. Schedule regular sessions.
Webinars	Attending live online workshops or seminars.	Interactive learning. Access to experts.	Fixed timing. Quality varies.	Webinar platforms. Attend live sessions and interact.
Internships/Apprenticeships	Learning on the job through internships or apprenticeships.	Real-world experience. Potential for job offers.	Unpaid or low pay. Quality of learning depends on the job.	Company websites. Apply for internships and complete assigned tasks.
Conferences/Workshops	Attending conferences or workshops related to your field.	Networking opportunities. Exposure to latest trends.	Can be expensive. Travel may be required.	Event platforms. Attend sessions and engage in discussions.
Online Forums/Communities	Participating in online forums or communities of learners.	Peer support. Diverse perspectives.	Quality of advice varies.	Reddit, StackExchange. Engage in discussions and ask questions.
Social Media Learning	Following influencers, joining groups or pages on social media related to your field.	Free. Informal learning.	Quality and reliability of information can vary.	LinkedIn Learning, Facebook groups. Follow, engage and participate in discussions.

Prepare a plan that works best for you. Things to consider:

Identify what learning options you have. There are various learning options for any IT or Cyber field. There are pros and cons to every option, which I have illustrated.

1. Time management for work-life balance
2. Time allocation for your job, social life, and learning security from the above options (Prepare a daily or weekly schedule, Set targets)
3. There are two ways you can create time table to try to follow it:
    a. Fixed time for your study in a day/week – This is suitable for people who know their weekly schedule, and they can dedicate a fixed time in a day/week to study.
    b. Fixed hours for your study in a day/week – This is suitable for people who do not have a fixed weekly schedule as they might have a shift job, on-call jobs or something else. So they can dedicate any slot for fixed 1/2/3 hours in a week.
4. Create study plan in Excel.
5. It is important to keep looking at it in order to follow it without fail so.
6. Stick it to your wall or any place which you cannot avoid looking at (e.g., Desk board, Refrigerator, etc.)

Enter the field

Perform a thorough **company research** before applying for a job.

Talking about reviewing a company, I would personally consider all factors before choosing my next company:

1. **Revenue –** To identify whether company is financially doing good or not.
2. **Company size –** To identify whether no. of employees are increasing or not. If increasing, company is doing great.
3. **Company's area of serving –** So you can predict what core values you would be serving to the company's wider level goal/business.
4. **Their client base –** So that you can understand who will be your most of the stakeholders with whom you will work on regular basis.
5. **Glassdoor and other reviews, Ppeople reviews –** Does not really matter, but may give you some indication of work culture especially the one with anonymous bad reviews and then you can ask around in your network to have better view of it before joining.
6. **Company Culture –** If you're curious about a company's culture, there are a few things you can look into. Check out employee reviews, take a peek at their social media channels, and pay attention to the language they use on their website. Are they all business and no fun? Or do they seem more laid-back and easygoing? Do they talk about valuing different perspectives and being inclusive? And what about taking care of their employees' well-being and giving them a good work-life balance? These are all clues that can help you get a sense of what it might be like to work there.
7. **Leadership –** If you want to learn more about the company, it's a good idea to look into the people in charge. Who is the CEO and what's their story? How long have they been working there? What's their leadership style like? You can usually find answers to these questions by doing a bit of online research, reading articles, and checking out employee reviews.
8. **Future Plans –** Are you curious about a company's future plans? It's always a good idea to research if they have a clear roadmap for the future, invest in new technologies or markets, or talk about their strong strategic plan publicly. You can often find this information by checking out employee reviews.
9. **Recent News and Events –** Look for any recent news articles or press releases related to the company. Has the company been in the news recently? If so, was the coverage positive or negative?
10. **Competitors –** Who are the company's main competitors? How does the company differentiate itself from these competitors? Understanding the competitive landscape can help you understand the challenges and opportunities the company may face.
11. **Company Values and Mission Statement –** Many companies post their values and mission statement on their website. Do these resonate with you? Do they align with your own personal values?

I believe below are the foremost common factors one should consider before selecting a company or applying for a role:
*There **can never be** any company which would fulfil all your below needs. (You will need to prioritize a minimum of 2 maximum 3 factors you would assess in your next company. So, if the first 2/3 of your needs are completed, you can select that company.)*

1. **Career advancement/Challenging work/Learning and development opportunities:** It's crucial to take into account the possibility of personal and professional growth in the position. Does the organisation prioritize the development of their staff? Are there chances to progress in one's career?
    a. **Example:** The company offers a range of programs to help their employees learn and enhance their skills, including certification sponsorship, conference/workshop attendance sponsorship, in-house training and development programs, and opportunities for cross-team learning.
2. **Base Pay/Salary/Bonus/Benefits:** When it comes to choosing a job, the compensation package, including salary, bonuses, and benefits, is an important factor to consider.
    a. **Example:** Companies offer discounts on general goods, insurance packages, annual bonus schemes, shares, holidays and other types of leaves, etc.

3. **Team/People/Boss/Management/Colleagues:** Your job satisfaction is greatly influenced by the quality of your team and managers.
    a. **Example:** Conduct thorough research on top and intermediate-level management personnel by browsing through LinkedIn and other social networks. Scrutinize their posts, content creation, and level of engagement to evaluate their personality traits. This will help you make an informed decision on whether or not to work with them in the future.

4. **Flexibility/Work-life Balance: With the rise of remote work, many values the flexibility to work from different locations or choose their working hours.**
    a. **Example:** Does the company provide remote work or flexible working days? How many days you can maximum work from home in a week? How many days/months you can maximum work from outside of your country? One of the great example is here - **https://jobs.netflix.com/work-life-philosophy**

5. **Type of company (Small, Big, Product based, Consulting based, Research-based, etc.)/Reputation/Brand: The type of company and its reputation can impact your work experience and future career opportunities.**
    a. **Example:** Working for Big4 consulting firms and FAANG companies can greatly add values to your resume. Research about the top companies in the world through it's sectors such as:
        i. **Info Tech –** Apple, Microsoft, Meta, Google, Amazon, Intel, AMD, Salesforce, Nvidia, Adobe, IBM, Cisco, ServiceNow, MSI, Qualcomm, HPE, Broadcom, etc.
        ii. **Healthcare –** UnitedHealth Group, Johnson & Johnson, Lilly, Pfizer, Abbott, Merck, Abbvie, Danher, Amgen, Medtronic, etc.
        iii. **Finance –** Berkshire Hathway, JPMorgan Chase & Co., VISA, Mastercard, Bank of America, Wells Fargo, Paypal, S&P Global, Citi, Aon, Blackrock, Goldman Sach, etc.
        iv. **Consumer –** Amazon, Macdonalds, Nike, TJX, The Home Depot, Ebay, Walmart, Pepsico, P&G, Cocacola, etc.
        v. **Industrial –** UPS, Honeywell, GE, Boeing, Lockheed Martin, etc.
        vi. **Communication –** Google, Meta, Netflix, AT&T, T-Mobile, Comcast, Walt Disney, Verizon, etc.
        vii. **Energy –** Exxon Mobil, Chevron, NextEra Energy, Duke energy, etc**.**

    To begin, it is important to compile a comprehensive list of industries within the market and identify the top 15 companies in each industry. This information can be organized using a spreadsheet in Excel. It is recommended to aim for a high-level position within your desired industry as a long-term goal.

6. **Type of Industry they serve (Banking/Financial, Retail, Gaming, Healthcare, etc.) /Reputation/Brand:** Matching your interest with a relevant industry can result in a more fulfilling career.
    a. Example: If you're passionate about gaming, companies like Electronic Arts or Ubisoft could be a great fit.

    Below is the list of all industries so far I know.
    Infotech, Healthcare, Logistics, Transportation, Gaming, Consumer, Industrial, Communication, Energy, Automotive, Aerospace, Agriculture, Biotechnology, Chemicals, Construction, Defense, Education, Electronics, Entertainment, Environmental Services, Fashion, Financial Services, Food and Beverage, Forestry, Hospitality, Insurance, Legal Services, Manufacturing, Mining, Oil & Gas, Pharmaceuticals, Printing and Publishing, Professional Services, Real Estate, Renewable Energy, Retail, Telecommunications, Textiles, Tourism, Utilities, Waste Management, E-commerce, Art & Culture, Fishing, Sports, Human Resources, Marine, Non-Profit, Online Media, Venture Capital & Private Equity, Research, Government, Public Relations, Security, Semiconductors, Shipping, Social Services, Space & Astronomy, Venture Capital and Private Equity, Wholesale, Design, Music

7. **Location: The proximity of the company may have an impact on your daily routine and travel time. However, with the rise of remote work, this aspect may not hold as much significance for certain individuals.**
    a. **Example:** If you work for a company based in a major city such as New York, London, Auckland, Mumbai, Delhi, San Francisco, etc., you can enjoy the perks of an exciting city life. However, this may come at the expense of higher living expenses and longer commute times.

8. **Types of services they offer: Understanding the company's product/service is essential, but its rank on the priority list may vary based on personal interest.**
    a. **Example:** Amazon Web Services (AWS) offers a broad spectrum of cloud services. If you're interested in cloud technology, this could be a compelling aspect of the job.

9. **Job Security: Especially in uncertain times, the stability of the industry and company is a crucial consideration.**

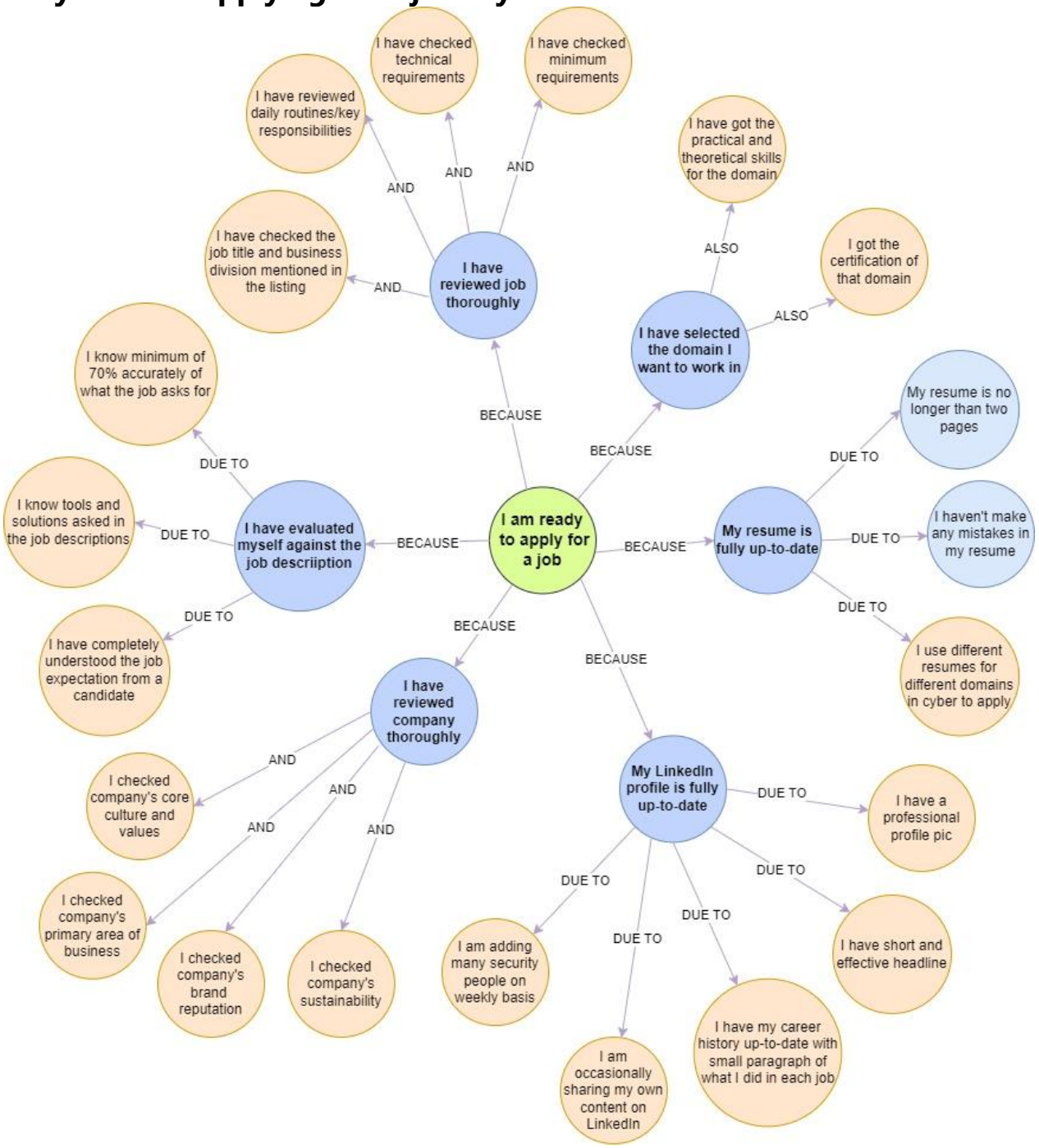
a. **Example:** Jobs in the healthcare industry, such as at a company like Johnson & Johnson, are often considered more stable compared to gaming industry or consulting industry. (This is just an example, not my opinion)

Find a quality mentor in cybersecurity

Finding the right mentor is challenging, especially for beginners in the security field. There are DOs and DON'Ts to consider before selecting the right mentor for yourself:

1. Don't just get attracted by no. of certifications those mentors have.
2. Don't select mentors just based on their online presence/appearance/how famous they are in the industry.
3. Don't select mentors just based on the total no. of experience they have.
4. Don't select mentors just based on their super technical hacking skills.
5. Don't select mentors just based on the number of achievements they possess.
6. Select a mentor who is down to earth, willing to learn from you as well while also coaching you.
7. Select a mentor who just not only solves your tech queries but gives you a perfect vision/direction for what you need to do to become XYZ down the line in the next 2-5 years and so on.
8. Select a mentor who is regularly contributing and giving back to the community.
9. Select a mentor with the right attitude not only the right knowledge.
10. Give time for your research, talk to them regularly, and talk to many regularly before you select them as your mentor.
11. Select more than one mentors even though their style of mentorship could be different, but it can greatly benefit you.
12. Make sure your mentor has the specific expertise or work experience in the area of cybersecurity you're interested in. For example, if you're keen on penetration testing, it would be beneficial to have a mentor who has hands-on experience in that field.
13. The mentor you select should be reasonably available to guide you. If they are too busy or not responsive, you may not be able to benefit from their knowledge and expertise. It's important to have a discussion about the frequency of meetings and the availability of time from both parties, whether on a weekly or monthly basis. Additionally, it's important to determine the preferred mode of communication, whether in-person or online. If online, it's important to specify the platform to be used.
14. Your mentor should be patient and understanding, as learning new skills often takes time. They should be able to offer constructive feedback without making you feel overwhelmed.
15. A good mentor can connect you with other professionals and resources in the field. This will not only expand your knowledge but also help you build your professional network.
16. A good mentor should inspire and motivate you. Their passion for the field should be evident, which in turn can spark your interest and keep you motivated.
17. Most notably, in the above list, ensure all or the majority of the points give a green signal to select your mentor and don't just evaluate anyone based on one or a few DOs or DON'Ts. Remember, no one is perfect in this world.

Only think of applying for a job if you have:



Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

Job hunting tips

If you are an experienced IT professional, you will need to tweak your resume to make it sound more of a cybersecurity one than just an IT.

If you are a beginner, you will require to create a professional resume to apply for a job. There are plenty of cybersecurity resume templates on Google that you can refer to.

If you have no professional experience in IT or Cybersecurity, you can add below things in your resume as a beginner. Kindly refer to the Resume writing – How not to blunder section.

Select any portal to apply for jobs but do not forget to use Google for jobs. Many jobs I have found on Google jobs portal which is not available on LinkedIn. Also Google jobs portal just extracts data from all various job portals.

You can contact specific cybersecurity recruitment companies who fill positions for big companies.

You can add cybersecurity-specific HRs to your LinkedIn to build relations and ask them to take an interest in your profile.

Prepare for interviews based on job descriptions. Whatever roles/responsibilities are mentioned in the JD, most likely, you will be asked questions from those areas only + some the things you have mentioned in your resume.

1. Understand each line of JD.
2. Give ChatGPT a little paragraph about the company information.
3. Then instruct ChatGPT to guess technical and scenario-based questions that can be potetntially asked to you once you supply full JD to it.
4. Get questions from ChatGPT and try to prepare answers.
5. Ensure you don't just mug up Q&A, you must have done that work practically even.
6. Understand each line of JD and try to find online labs/resources to learn. E.g., TryHackme.
7. Practice it practically.
8. Try to evaluate what soft-skill-based questions can be asked and be ready to answer with specific examples.

Congratulations! Mission NOT Completed.

It is not over yet. You have just entered the cybersecurity world. There are things you will need to continue doing for better survival and better growth.

1. **Learn more things –** Learn those things in your company which you cannot simply learn by Google and YouTube. E.g., One can learn how to hack a website by sitting at home, but cannot learn, how to design a new secure architecture diagram for application development within the DevSecOps project based on their company's infrastructure. That is the real experience.
2. **Advancing to management –** See what else you would require learning apart from tech skills to advance your career to the management level. Learn more soft skills in business, and management. Learn people, process and technology problem dealing.
3. **Know your competitions –** Competitions are everywhere; it is an excellent way to keep yourself motivated and learn more things that others are learning in your network.
4. **Know the market –** Understand how the market is shifting in cybersecurity, know various new vendors coming into the market, and launching their products to tackle large enterprise problems. Understand what problems are being discussed in the community through conference panel discussions, YouTube podcasts, or other sources. Understand the market when you started your career, how rapidly it is changing, and where it is going. You can determine your future roles and opportunities and can set goals accordingly.

5. **Do not get demotivated –** Cybersecurity is a very competitive field. You will meet many people in your life who might know more things than you. Don't get demotivated by that. If they know 2 things, you know 1; if they share 1 extra thing with you, now you both know 2 things. So always keep +ve attitude of learning from them and don't get demotivated by your position of learning.
6. **Make StackOverflow, ChatGPT & Google your besties –** It is not important what you don't know; it is crucial to how quickly can you learn. Google and StackOverflow are the best sources for your doubts (tech or non-tech). Keep them at your fingertips. It is ok to ask stupid questions, so keep asking around.
7. **Community appearance –** You should attend/present at well-known conferences. Start with your local town conference/meetups. Present on a few topics. Gain confidence in public speaking. Then advance to national level conferences and then international level. Meet more people and build relationships.
8. **Bad practices in Cybersecurity –** Nothing is perfect in this world. In cybersecurity, even there are bad practices, loopholes, and cheats. Ensure whatever small or big decision you take; you do all your sanity checks and don't get training to all of these.
9. **Work on Your Communication Skills -** Whether it's writing an email, presenting a project, or just daily conversation, effective communication is crucial in the workplace. The better you are at conveying your ideas, the more impact you'll have.
10. **Mentorship -** Seek out mentors within your industry. These individuals can provide guidance, offer advice, and help navigate your career path. Similarly, be willing to mentor those who are newer or less experienced than you. This can be a rewarding experience that also improves your leadership skills.
11. **Maintain a Healthy Work-Life Balance -** This one often gets overlooked, but it's crucial to your long-term success and mental health. Make sure to take time for yourself and your loved ones. Exercise, hobbies, and relaxation are just as important for your career growth as your professional development.
12. **Professional Certifications -** Earning professional certifications in cybersecurity can be very beneficial in expanding your knowledge and skills, and it could also make you more attractive to employers. Certifications like CompTIA Security+, Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), etc. can give you an edge in your career.

As a beginner, what all fundamentals I should learn?

For those new to the field, the prospect of beginning a career in cybersecurity can be daunting. The sheer variety of specializations and sub-fields can make it challenging to know where to begin. My recommendation is to start by developing a foundational understanding of each area of cybersecurity and then exploring opportunities to apply that knowledge across multiple domains. By keeping your options open in this way, you may find it easier to secure a job in the field. To help you get started, I have compiled a list of the major areas of cybersecurity and the resources you'll need to begin learning about them. I encourage you to take advantage of these resources and start building your knowledge base today!

Area	Technical Skills	Soft Skills	Sub-domain	Learning Approach	Resources
Fundamental Concepts	Understanding of cybersecurity basics: confidentiality, integrity, availability (CIA); threat modeling;	Critical thinking, ethics in cybersecurity, communication skills	Information Security Management, Risk	Study key cybersecurity principles and frameworks;	Cybrary, OWASP

	risk assessments; cybersecurity frameworks (NIST, ISO 27001)		Assessment, Cybersecurity Audit	Participate in online cybersecurity communities	
Computer Networks	Network protocols (TCP/IP, HTTP/HTTPS, DNS); network infrastructure (firewalls, routers, switches); network security (intrusion detection systems, secure network architecture)	Understanding the business impact of network security, team collaboration	Network Security, Intrusion Detection, Secure Network Design	Get certifications like CCNA, Network+; Build home labs for practical experience	Cisco Networking Academy, CompTIA Network+
Cryptography	Symmetric and asymmetric encryption; hash functions; digital signatures; public key infrastructure (PKI)	Understanding the legal and ethical implications of encryption, strong attention to detail	Encryption, Cryptanalysis, PKI Management	Study cryptography principles, understand real-world applications; practice encrypting and decrypting messages	Crypto101, Coursera Cryptography Course
Software Security	Secure coding practices; understanding common vulnerabilities (SQL injection, buffer overflow, cross-site scripting); static and dynamic analysis	Ability to communicate the business risks associated with software vulnerabilities, patience and diligence	Secure Development, Vulnerability Assessment, Penetration Testing	Learn secure coding; Participate in Capture The Flag (CTF) challenges	OWASP WebGoat, Hack The Box
System Security	Understanding of operating systems security features; system hardening; patch management; endpoint protection	Understanding the cost and business impact of system downtime, prioritization	System Hardening, Endpoint Protection, Access Control	Get certifications like CompTIA Security+; Practice system hardening on virtual machines	Microsoft Learning, CompTIA Security+

Cloud Security	Understanding of cloud-based technologies (AWS, Azure, Google Cloud); virtualization; container security; cloud security architecture and tools	Understanding cloud security governance, risk management and compliance (GRC), contract negotiation	Cloud Architecture, Cloud GRC, DevSecOps	Get cloud-specific certifications like AWS Security, Azure Security Engineer	AWS Training, Microsoft Learn
Incident Response	Incident detection, analysis and response; digital forensics; remediation	Crisis management, strong communication skills, decisiveness	Incident Management, Digital Forensics, Disaster Recovery	Participate in incident response drills; Get certifications like Certified Incident Handler (ECIH)	SANS Institute, EC-Council
Threat Intelligence	Analyzing threat trends; understanding threat actors and their tactics, techniques, and procedures (TTPs); knowledge of various intelligence sources	Analytical thinking, communication skills, situational awareness	Threat Analysis, Strategic Intelligence, Tactical Intelligence	Learn the cyber threat landscape, follow cybersecurity news, practice analyzing threat reports	MITRE ATT&CK, Threatpost
Data Security	Understanding of data lifecycle, data encryption, data loss prevention (DLP), privacy regulations (GDPR, CCPA)	Understanding business value of data, ethical considerations	Data Governance, Privacy Compliance, Data Loss Prevention	Learn about privacy laws and regulations, understand DLP tools	International Association of Privacy Professionals, Coursera - GDPR
Physical Security	Knowledge of secure facility design, access control systems, surveillance systems	Understanding of risk management, interpersonal skills	Facility Security, Surveillance, Personal Security	Gain a broad understanding of physical security principles, learn	ASIS International, Security Management

				how physical and cyber security overlap	
Mobile Security	Understanding mobile OS architecture, mobile malware, mobile application security	Understanding the implications of mobile device loss, patience and diligence	Mobile Device Management, Mobile Application Security, Mobile Threat Defense	Learn about mobile OS, app vulnerabilities; Test apps in controlled environments	OWASP Mobile Security Project, Mobile Security Framework
Social Engineering	Understanding of phishing techniques, pretexting, baiting, tailgating	Strong understanding of human behavior, critical thinking	Phishing Simulation, Awareness Training, Social Engineering Penetration Testing	Learn how to identify common social engineering tactics; Awareness Training	Social Engineer, KnowBe4
Governance, Risk, and Compliance (GRC)	Understanding of cybersecurity policies and procedures, risk assessment methodologies, legal and regulatory requirements	Strategic thinking, strong communication skills, business acumen	Cybersecurity Governance, Risk Management, Compliance	Study for certifications such as CISM, CRISC; Understand business requirements and align security with them	ISACA, IT Governance Blog
Penetration Testing	Knowledge of penetration testing methodologies (OWASP, PTES); understanding of vulnerabilities and exploits; proficiency in penetration testing tools (Metasploit, Burp Suite, Wireshark)	Critical thinking, attention to detail, report writing	Web Application Penetration Testing, Network Penetration Testing, Mobile Application Penetration Testing	Learn penetration testing methodologies; practice in lab environments; acquire certifications like OSCP, CEH	Penetration Testing Execution Standard, OWASP Testing Guide, Offensive Security

Red Teaming	Knowledge of advanced penetration testing techniques; familiarity with threat emulation; understanding of social engineering and physical security	Strategic thinking, adaptability, team collaboration	Advanced Persistent Threat Emulation, Social Engineering, Physical Intrusion	Gain experience in penetration testing; participate in red team exercises; acquire CRT (Check Red Team) or similar certifications	Red Team Journal, Red Teaming/Adversary Simulation Toolkit
Security Operations Center (SOC)	Understanding of SIEM tools (Splunk, QRadar); knowledge of intrusion detection and prevention systems; incident response	Ability to work under pressure, strong communication skills, analytical thinking	L1 Analyst (Monitoring and Triage), L2 Analyst (Incident Response), L3 Analyst (Threat Hunting)	Work in a SOC environment; get certifications like CompTIA CySA+, EC-Council Certified Incident Handler	SANS Blue Team Fundamentals, Splunk Fundamentals

Roles and Responsibilities *(Source: TryHackMe)*

Role	Description	Responsibilities
Security Analyst *(Responsible for maintaining the security of an organization's data)*	Security analysts are integral to constructing security measures across organizations to protect the company from attacks. Analysts explore and evaluate company networks to uncover actionable data and recommendations for engineers to develop preventative measures. This job role requires working with various stakeholders to gain an understanding of security requirements and the security landscape.	• Working with various stakeholders to analyze the cyber security throughout the company • Compile ongoing reports about the safety of networks, documenting security issues and measures taken in response • Develop security plans, incorporating research on new attack tools and trends, and measures needed across teams to maintain data security.
Security Engineer *(Design, monitor and maintain security controls, networks, and systems to help prevent cyberattacks)*	Security engineers develop and implement security solutions using threats and vulnerability data - often sourced from members of the security workforce. Security engineers work across circumventing a breadth of attacks, including web application attacks, network threats, and evolving trends and tactics. The ultimate goal is to retain and adopt security measures to mitigate the risk of attack and data loss.	• Testing and screening security measures across software • Monitor networks and reports to update systems and mitigate vulnerabilities • Identify and implement systems needed for optimal security
Incident Responder/Digital Forensics	Incident responders respond productively and efficiently to security breaches. Responsibilities include creating plans, policies, and protocols for organisations to enact during and following incidents. This is often a highly pressurized position with assessments and responses required in real-time, as attacks are unfolding. Incident	• Developing and adopting a thorough, actionable incident response plan • Maintaining strong security best practices and supporting incident response measures

(Identifies and mitigates attacks whilst an attacker's operations are still unfolding)	response metrics include MTTD, MTTA, and MTTR - the meantime to detect, acknowledge, and recover (from attacks.) The aim is to achieve a swift and effective response, retain financial standing and avoid negative breach implications. Ultimately, incident responders protect the company's data, reputation, and financial standing from cyber-attacks. If you like to play detective, this might be the perfect job. If you are working as part of a law-enforcement department, you would be focused on collecting and analysing evidence to help solve crimes: charging the guilty and exonerating the innocent. On the other hand, if your work falls under defending a company's network, you will be using your forensic skills to analyse incidents, such as policy violations.	• Post-incident reporting and preparation for future attacks, considering learnings and adaptations to take from incidents • Collect digital evidence while observing legal procedures • Analyse digital evidence to find answers related to the case • Document your findings and report on the case
Malware Analyst *(Analyses all types of malwares to learn more about how they work and what they do)*	A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings. A malware analyst is sometimes called a reverse-engineer as their core task revolves around converting compiled programs from machine language to readable code, usually in a low-level language. This work requires the malware analyst to have a strong programming background, especially in low-level languages such as assembly language and C language. The ultimate goal is to learn about all the activities that a malicious program carries out, find out how to detect it and report it.	• Carry out static analysis of malicious programs, which entails reverse-engineering • Conduct dynamic analysis of malware samples by observing their activities in a controlled environment • Document and report all the findings
Penetration Tester *(Responsible for testing technology products for security loopholes)*	You may see penetration testing referred to as Pentesting and ethical hacking. A penetration tester's job role is to test the security of the systems and software within a company - this is achieved through attempts to uncover flaws and vulnerabilities through systemised hacking. Penetration testers exploit these vulnerabilities to evaluate the risk in each instance. The company can then take these insights to rectify issues to prevent a real-world cyberattack.	• Conduct tests on computer systems, networks, and web-based applications • Perform security assessments, audits, and analyse policies • Evaluate and report on insights, recommending actions for attack prevention
Red Teamer *(Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective)*	Red teamers share similarities to penetration testers, with a more targeted job role. Penetration testers look to uncover many vulnerabilities across systems to keep cyber-defense in good standing, whilst red teamers are enacted to test the company's detection and response capabilities. This job role requires imitating cyber criminals' actions, emulating malicious attacks, retaining access, and avoiding detection. Red team assessments can run for up to a month, typically by a team external to the company. They are often best suited to organisations with mature security programs in place.	• Emulate the role of a threat actor to uncover exploitable vulnerabilities, maintain access and avoid detection • Assess organizations' security controls, threat intelligence, and incident response procedures • Evaluate and report on insights, with actionable data for companies to avoid real-world instances
Security Analyst (SOC – Tier 1) *(Triage)*	A Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring a company's network and systems 24 hours a day, seven days a week. Their purpose of monitoring is to: • Find vulnerabilities on the network • Detect unauthorized activity • Discover policy violations • Detect intrusions	As Tier 1 analyst in the SOC, your duties will involve • Monitor network traffic, logs, events, alerts • Work on tickets and close, triage alerts • Perform basic investigation & mitigation,

Security Analyst (SOC – Tier 2) *(Incident Responder)*	A Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring a company's network and systems 24 hours a day, seven days a week. Their purpose of monitoring is to: • Find vulnerabilities on the network • Detect unauthorized activity • Discover policy violations • Detect intrusions	As Tier 2 analyst in the SOC, your duties will involve • Focus on the deeper investigation, analysis and remediation. • Proactively hunt for adversaries • Monitor and resolve more complex alerts • Prepare weekly/monthly reporting
Security Analyst (SOC – Tier 3) *(Threat Hunter)*	A Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring a company's network and systems 24 hours a day, seven days a week. Their purpose of monitoring is to: • Find vulnerabilities on the network • Detect unauthorized activity • Discover policy violation • Detect intrusions	As Tier 3 analyst in the SOC, your duties will involve • Works on more advance investigations & remediation • Perform advance threat hunting and adversary research by consuming threat intel data • Malware analysis and possible reversing • Developing new adversary detection signatures through SIEM

Master's Degree

Shall I go for a master's degree?
Shall I go for master's in your own country or foreign?
Is there any value in a master's degree?

Let me start answering this section with myths and realities.

Myths	Reality
A Master's degree in cybersecurity is not required.	It is true but not 100%. There are some intermediate benefits of having a master's degree on your resume. Those benefits are not just limited to your technical and academic knowledge of cybersecurity but also related to your people networking and other soft skills such as team building, project management, strategic planning, communication, business communication writing, etc.
A Master's degree in cybersecurity is helpful to get more salary or a quick job.	There won't be any difference in your starting salary as a fresher in cybersecurity even though you have a masters from any country. There is an exception to this. If your university is super famous and has quality placements, then based on grad assessments, they can give you a good package as a starter compared to someone who just passed out from university and is trying to find a job via LinkedIn and other portals.
Cybersecurity requires skills, and masters, they don't teach practical knowledge; they only teach basic skills and primarily theoretical.	It is not true, and it is based on the university to university and country to country. What you see people doing in the community is knowledge of working in corporate & doing professional research. Don't expect the university will provide you with that level of knowledge.

	Master's programs are designed to develop your cyber foundation and let you know how many different fields there in cybersecurity are rather than teaching you very professional stuff that is being used in the corporate world. They expect you to clear your fundamentals, communication, and consulting skills. Also, if you are a university pass out, companies understand your level of knowledge, so they will not even expect you to showcase your skills that match their company's requirements.
If I have masters in cybersecurity, my chances of getting selected for job interviews are higher	It won't make any difference in job interviews; people with even CA or commerce with cyber knowledge and skills can get a job instead of you. This field demands skills and knowledge and not your solid academic background only.

The first thing to consider is why you want to study for a master's in the first place. Is it so that you can progress in your career? Is it a requirement to pursue a particular field? Or are you just doing it for the sake of learning? Whatever the reason, it can help you to narrow down your options. Don't be tempted to pick a degree just because you feel it might look good on your CV, either.

This question is very hypothetical, and there is not a single answer. There are 50-50% advantages and disadvantages of doing and not doing a master's in your career, especially in cybersecurity or any other field.

Advantages:

- If you do a master's degree in foreign country, you will get good local exposure to that country; you will be studying and spending time with different people from various countries.
- Your communication will be improved.
- You will be doing many projects with your classmates together, which will teach you how professional project management can be done, including planning, execution, communication, & presentation.
- You will be able to travel to a new country to meet new people, get exposure to the local cybersecurity market of that country, regional security conferences, etc.

Disadvantages:

- A Master's degree will not give you real-life knowledge of security that is being done in corporates. However, this is not a big disadvantage, as those programs are designed to build a foundation only.
- A Master's degree takes 2/3 years of your life. So, if you want to skip it, you can have 2/3 years of corporate experience instead of doing masters.
- Masters will not give you a higher salary.
- Masters will not make you different in job interviews.
- Course fees are very high, especially you if are going for a master's degree in western countries.
- **Important:** You may or may not get a post-study work visa. In most countries, once you study, there are very tiny chances of finding a company that can sponsor you, so you may have to come back to your original country after studying there. Work visa sponsorships are very, very, very rare for Indian students.

So, it really depends on you. If you have TIME and MONEY and want to get some foreign exposure, you can do master; else, you can prefer doing it from your own country. If you don't have time and money, you can skip it and get a job directly after your bachelor's.

Things to consider before choosing any master's degree program
Post-study work visa options/Chances of sponsorship
Course syllabus and topics of study
Professor's background and credentials

University's global rank and national rank
University's partnership with leading security firms/government agencies
Internship opportunities are included or not
Post-study placement opportunities are included or not
Access to the career services department has been in helping you prepare for interviews and search for internships and full-time jobs
Consider course fees
Consider course duration/length
The job market in the country you are planning to do masters

Internship

Shall I go for an internship in any company after my study?
Will it be helpful in my career?
What kind of internship do companies provide?
Is it necessary to do it from a renowned company or any company?

The answer to this question is too broad. It depends on many factors such as:

- Which company is providing Internship (Product based company, security consulting company, Big4 etc.?)
- What are their requirements for internship programs?
- What will be the job roles and responsibilities during the internship?
- What are the expectations from an employer?

There are very few; I would say only a handful of companies that provide quality internships where you would learn valuable things. Most of the money-making companies are running CEH (Certified ethical hacker – Which is the official certification from EC-Council, a well-reputed cybersecurity certification authority) and related courses on the name of an internship. For example, if my company's name is Prakash, then I will provide my own CEH certification in the name of "PCEH – Prakash Certified Ethical Hacker" and so on.

So, I have prepared 'DO' and 'DON'T' for selecting a company for your internship.

DO
Understand the nature of a company (consulting, product-based, small, big, etc.).
Ask them about your daily responsibilities, tasks, and job routines.
Ask them what the learning options are they can provide to you during your internship.

Ask them what their expectations from you during the duration of the internship will be.
Ask more and more people around for the reviews of those companies you are evaluating for internships.
Identify your career interests. This could be done by self-reflection, speaking with a Career Counsellor or your mentor
Ask the company about paid or unpaid Internships. You can go for any as far as other criteria are matched.
Start searching for an internship at least 6 months prior.
If you are interested in any company and can't find any internship opportunity, you can check their website and social media. Connect to their HRs via LinkedIn and ask the same.
Better understand and research who they are, what they do, their strengths and weaknesses
Perform at least 5 mock interviews with your career counsellor or mentor before going for an internship interview.
DON'T
Don't select a company that just provides course teaching, coaching.
Don't select a company that do not serve any clients or serve any handful of clients only with simple projects.
Don't select a company that asks you to teach their students via their coaching, training programs.
Don't get attracted by any company's marketing & PR success.
Don't get attracted by their company's reputation through magazines, press, awards from random conferences or panels.
Don't select a company where only 4/5 people are working; all are Founders, Co-Founders, Directors. If you do, please check their professional background. Check whether they obtained these titles without having any prior corporate experience or started their start-ups after having at least 8 years of experience in the industry.

Which certifications should I go for?

This is a debatable question, and there is definitely not a single answer for this. Before planning for the certifications, it is best to know what the factors are to consider before choosing/going for any certification.

Things to consider before choosing any cybersecurity certification
Certification must be from well-known authorities
Cybersecurity-specific cert provider authorities - ISC2, eLearnSecurity, Offensive Security, ISACA, EC-Council, CompTIA, CREST, SANS, GIAC, etc.
These are vendor product-specific cert provider authorities – Amazon (AWS), Google (GCP), Microsoft (Azure), Cisco, Checkpoint, etc. There can be others as well.
Are these certs requiring in the market? Search LinkedIn jobs where those JDs require these certs for the jobs. If they are not required, no need to go for that cert
Are you going for a beginner level cert in your particular domain or going for a management/high-level cert directly? Know what the starting point vs is ending point
Are you going to obtain multiple certs from the same cert provider or choose different cert providers every time? It is good to have different cert providers' certificates on your resume.

Are you taking cert for the sake of job only? Or for knowledge? If the job only then is, you are spending a huge amount of money without having any job confirmation even?
What will be the future of this cert after 5 years? Can it be obsolete? Will people still feel its value? E.g., the Overtime value of CEH has dropped, companies still recommend it, but anyone who has CEH is not that regarded compared to OSCP, OSCE, GPEN, etc. E.g., Regardless of the time period, the value of CISSP, Security+ have always been there in any company. It has never decreased.
Are your career goals aligned with the certificate you are going to obtain?
If possible, it is recommended to obtain a certificate in technical and managerial areas of your cybersecurity domain.

Types of companies

How many types of different companies are there?
Which types of companies to choose in the initial career?

Legends	Consulting (Big4 & Other Big companies)	Small Consulting Firms	Product-based Firms	Security Vendor Firms
Size	They are giants, thousands of employees	Small and Medium Enterprises	It can be any small, medium, large Enterprises	It can be any small, medium, large Enterprises
Reputation	Well-reputed	Maybe reputed in their region (State or city) Sometimes famous within the country but not internationally reputable and known	Can be well-reputed within a country or internationally recognizable.	Can be well-reputed within a country or internationally recognizable.
Example	KPMG, Deloitte, EY, PwC, Accenture, etc.	Your local security consulting firms.	Google, Microsoft, Apple, Amazon, Tesla, Walmart, etc. Your local product-based companies are smaller than the above giants.	All cybersecurity vendors: CrowdStrike, Whitehat, Rapid7, Qualys, Tenable, RSA, Trustwave, Imperva, etc.
Client-base	Serves clients all over the world	Limited based on their presence, areas of services they provide due to expertise	Big giants serve the entire world. Small companies are limited to serve their local clients.	Big giants serve the entire world. Small companies are limited to serve their local clients.
Project type	Executes various types of projects (Projects vary from technical to management all areas of cybersecurity)	Depends on the areas of services they master. They will provide services in limited cybersecurity areas based on their expertise. Some only provide technical, some provide tech + management, etc.	You will be doing anything and everything to secure the products of these companies from external attackers.	Two types of roles: 1. Serve clients by solving their queries on your security products OR 2. Work with the engineering team to enhance product algorithm, engine, features, signatures.

Learning opportunity	Good learning opportunities in consulting & technical both areas. Their own global network cross-country learning opportunities	Limited (From your peers and surroundings) Mostly, you will be a self-learner	Massive as you work within a company to secure their infrastructure. So, you have the advantage of knowing the company better than external attackers.	Limited based on the area you work in for that firm.
Your role	Jack of all trades	Jack of all trades but limited to one domain of cyber. If Pentesting, then all Pentesting areas only.	You will be required to work within 1 or 2 domains of cybersecurity within that company, and there will be other security domains. You work closely with every team to secure your company's products.	Master of one (You will be working in a limited cyber domain, but you will be master of that domain)
Salary	Competitive salaries	It depends on the size and revenue of the organization	Competitive salaries (depends on the size of the company)	Competitive salaries (depends on the size of the company)

Resume writing – How not to blunder

Do you want to break into cybersecurity but don't have the experience to show on your resume?

No worries.

Here are ten great resume-building activities that will make you stand out from the competition: (Thanks to Naomi Buckwalter for compiling this list - https://www.linkedin.com/in/naomi-buckwalter/)

1. Volunteer with a cybersecurity conference
2. Teach a cybersecurity class
3. Mentor a student
4. Join a cybersecurity working group
5. Contribute to an open-source project
6. Build a home lab
7. Start a blog
8. Guest on a podcast
9. Lead a study group
10. Start a cybersecurity meetup or club
11. Get a basic CEH, Security+ or equivalent cert
12. AWS, Azure, GCP, etc. certifications
13. Find a vulnerability in a reputed website (bug bounty)
14. Find zero-day and get a CVE id

Once you do the majority of these, you would have a good number of things to showcase in your resume and your Interview.

Below are some common resume blunders I have seen over the years. Try to avoid it.

Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

Resume Blunders to Avoid	
Typos and Grammatical Errors	It's crucial to proofread your resume before submitting it. Errors may suggest a lack of attention to detail or professionalism.
Providing Inaccurate Information	Whether it's wrong dates or exaggerated qualifications, falsifying information is always a big no-no.
Using an Unprofessional Email Address	Your email address should be simple, professional, and easily identifiable as yours. Avoid using inappropriate or quirky email handles.
Including Personal Information	Details about your age, religion, marital status, and other personal data should not be on your resume, as they could lead to unconscious bias or even legal issues.
Having an Objective That's Not Related to the Job	If you include an objective, it should directly relate to the position you're applying for.
One-size-fits-all Resumes	Tailor your resume to the specific job you're applying for. Highlight the most relevant experiences and skills.
Overloading Your Resume	Keep your resume concise. Typically, a resume should not exceed two pages. Too much text can be overwhelming and important information may be overlooked.
Listing Responsibilities Instead of Achievements	Employers are more interested in what you've accomplished in your roles than a list of duties.
Including Irrelevant Information	Hobbies, interests, and experiences that do not relate to the job you're applying for should not be included.
Not Using Action Verbs	Use strong action verbs to begin your bullet points to give them more impact.
Using Clichéd Buzzwords	Terms like "synergy", "go-getter", and "team player" are overused and have lost their impact. Be specific about your skills and accomplishments instead.
Lack of Specifics	Vague statements do not help employers understand your abilities. Be specific and offer details about your accomplishments.
Poor Formatting	Avoid using unusual fonts, colors, or graphics. Stick to a clean, professional format.
Including References on Your Resume	Unless specifically asked, you don't need to include references in your resume. The phrase "references available upon request" is also unnecessary.
Outdated Information	If it's not recent or relevant, consider whether it really needs to be on your resume.
Not Using Numbers	Quantifying your achievements can help give a clearer picture of your capabilities and impact.

Using an Inappropriate Resume File Name	The file name should be professional and make it clear whose resume it is.
Having an Unfocused Career Objective or Summary	If included, these should clearly communicate your career goals and why you're a good fit for the position.
Excessive Jargon or Acronyms	Not everyone reading your resume may understand industry-specific terminology, so it's best to avoid or explain it.
Inconsistent Tense	Use past tense for past jobs and present tense for your current job.
Long Paragraphs	Instead of writing long paragraphs, use bullet points to make your resume easier to read and understand.
No Clear Structure	Your resume should have a clear structure with headers, bullet points, and consistent formatting.
Using "I" or "My"	It's better to use third-person or no pronouns at all in your resume.
Not Highlighting Promotions	If you were promoted in a company, it's important to highlight this to show your success and progression.
Not Aligning Resume and LinkedIn Profile	Your resume and LinkedIn profile should complement each other and present a consistent narrative about your career.
Lack of Contact Information	You'd be surprised how many people forget to include their contact information. Make sure to include your phone number and professional email address.
Including a Picture	Unless you are applying for a job where your appearance is important (like acting or modeling), there's no need to include a picture. It could potentially lead to discrimination.
Not Including a Cover Letter	Although it's not always required, including a cover letter can provide context and personality that your resume might not be able to convey.
Not Showcasing Transferable Skills	Especially when changing industries or roles, it's important to highlight skills that can transfer from one job to another.
Irrelevant Job Experience	Unless you can demonstrate how an older or unrelated job helped develop your skills for the job you're currently applying for, it's usually best to leave it off your resume.
Missing Keywords	Many companies use automated applicant tracking systems (ATS) that look for specific keywords related to the job. If your resume doesn't have those keywords, it might be overlooked.
Overusing Bold or Italic Text	Use bold and italic text sparingly to highlight important parts of your resume. Overuse can make it look cluttered and unprofessional.

No Hyperlinks to Professional Online Profiles	Including hyperlinks to your LinkedIn profile or online portfolio can provide more context and depth to your resume.
Including High School Information	Unless you're a recent high school graduate, there's no need to include high school information. Focus on more recent and relevant education and experience.

LinkedIn – Why create a quality profile

One question to you, do you want to get noticed by reputable persons in your industry? Then it is a must to create a killer LinkedIn profile. Here are the steps to create and maintain a perfect LinkedIn profile.

How to create a killer LinkedIn profile	
Profile pic	Your profile picture matters a lot to many. It's not about to look, but it's about professionalism. We have social media like Facebook, Instagram, etc., to share our photos in whichever way we want. But on LinkedIn, many HRs or professionals would want to see you as a professional. Posting a professional profile pic shows your attitude, how seriously you take a LinkedIn platform, and professionalism. Not that it's going to affect you a lot in your next Interview round, but something to consider in order to mature your LinkedIn profile from all 360 degrees.
Things you share and like	Things you share and like describe your personality. This is a very common issue among all. People share and like a random post. People use LinkedIn from their perspective but not from the other's (HR and big company's CEO or manager) perspective. Ask yourself if you are HR and if you want to find a candidate to work in your company, and you are visiting his or her profile. You find more stuff regarding other general things such as jokes, politics, random debates, inspirational quotes etc. How would you know that the person is good at his domain or not? Does that profile sound good? If you are a cybersecurity person and visit my profile, there should be some takeaway for you in terms of my knowledge sharing through my profile. So, you visit my profile, and you will find more articles, links, etc., about cybersecurity that may interest you. Because this is a professional network, and you should try to share and like stuff related to your profession only. So, the point is only talking about shares and likes related to your field, not random things.
Writing a post on your wall	Writing a post also matters a lot. Do not write stuff out of your field, portraits discrimination, hate rate, bad things about a specific community, cast, religion, etc. Your post must be crystal clear and should be understood by all types of audiences who read it. Don't do bulk sharing. You shared a post today; wait for 5 days at least to write another post. Let people read, react like and share your existing work. Don't act like a spammer or unprofessional enthusiast who just keep on sharing things to increase your reachability.
Write relevant posts	Only write posts that are not discussed before yet not explored a lot. Well, I would never talk about cybersecurity, why it is essential, what is website hacking, etc. Numerous amounts of the stuff are there on the internet. I would only discuss specific things within the topic only, which can take the interest of others. If I sound unique, people may create an impression that I am a researcher/explorer, not just a techie guy who works on cybersecurity. Writing a post can be your own work, discussion topic, research, tutorial, literature review and debate outcomes. Always before writing, think that do I sound negative? Can many people dislike this, or do I have a negative view of this topic compared to others? Do not share such things at all. You must be neutral on each topic. Be neutral, be unique, add more specific and detailed things to explain your writing, give a clear message do not sound confused that whether you are asking or telling or just sharing or what you want, avoid using short forms and F words or any lame and abusing words.
Be polite and gentle	Be gentle all the time. When someone adds you give these two lines to them. Thanks for adding me to your professional network. I am glad to connect with you. How are you? No need to use sir, mam; no one likes that on LinkedIn. If you share something and people give negative comments, then gently accept, or share your further argument. Do not fight. Choose your words carefully.

Contact information	Keep your LinkedIn profile up to date with your contact info, email id, phone number and other details. For your every job, also mention what your key role in that company was. Also, mention if any awards or recognition you got in that company or not. For this, you can visit my profile and check yourself how I highlighted my work in each former company.
Introduction Paragraph	Write your introduction paragraph carefully, mention three things. What are you? No. of experience and what are you looking for in your future (means where you want to move your career ahead, what you want to learn, what type of challenging roles you are looking for)
Achievements	Mention the relevant achievements in your profile only. I have plenty of national-level prizes in drawing competitions but does it relevant to my profile. HR is visiting my profile to see what kind of tech expertise I have. How does it matter to them? Even within IT, I hold web and graphics designing certification from Aren animation. Still, I work on cybersecurity, so I don't see a reason to share this even in my profile. So only share relevant things.
Profile title	Add the best profile title. 2 liner title. Whoever visits your profile, he/she should have your impression just by looking at your profile title only. For this, visit my profile and see how and what I wrote under my name.
Upload documents	Add images or documents to your experience. Did you know that you can add media files to your experience? It is a great way to create a visual portfolio along with your standard resume information.
Ask for recommendations	Endorsements are great, but recommendations are the currency of the realm on LinkedIn. Reach out to past colleagues, managers, and associates and ask that they write you a recommendation.

Finding a job in a foreign country

How to get a job in a foreign country?

It is hard to get a job in a foreign country sitting in your own country. Why because of Visa sponsorship.

Visa Issues: One of the major obstacles that many international students face when seeking employment is their visa status. Companies might be reluctant to hire someone who requires sponsorship for a work visa due to the additional cost and paperwork involved. Also, there can be uncertainties around the length of stay the visa allows.

Local Experience: Some employers may prefer candidates who have previous work experience in the country, as they would be more familiar with local industry practices, regulatory environments, and cultural norms. This can put international students at a disadvantage, especially if they don't have any local work experience.

Cultural Differences: Even with the right skills and qualifications, cultural differences can impact a candidate's ability to fit into the workplace. These could include language barriers, communication styles, and understanding of local customs and etiquette.

Networking: In many industries and countries, a lot of jobs are found through networking. International students may lack this local network which makes it more difficult for them to learn about job opportunities.

Among all above, VISA is the biggest factor. Let's understand that in detail:

In the UK, an international candidate usually needs to have a Tier 2 (General) visa to work. For a company to hire such a candidate, they generally need to do the following:

1. **Obtain a Sponsor License:** Before a company can employ someone from outside the UK, they generally need to be licensed to sponsor international workers by the Home Office. This involves an application process, during which the company must demonstrate that they are a genuine organization operating lawfully in the UK, and that they are aware of and capable of carrying out their sponsorship duties.
2.
3. **Issue a Certificate of Sponsorship:** Once the company has a Sponsor Licence, they can issue a Certificate of Sponsorship (CoS) to the individual they wish to hire. This is not a physical document, but a unique reference number that the candidate will need when they apply for their visa.

4. **Carry out a Resident Labour Market Test (RLMT):** Before they can issue a CoS, the company generally needs to demonstrate that they've made a genuine effort to fill the position with a resident worker. This often involves advertising the job in the UK for a certain period and documenting the recruitment process. As of my knowledge cutoff in 2021, the RLMT requirement has been replaced by a points-based immigration system, but employers still need to demonstrate that the job is at an appropriate skill level and that it pays a suitable salary.

5. **Manage Ongoing Sponsorship Duties:** Once the individual is employed, the sponsoring company has a range of ongoing duties to fulfill. These can include keeping records on the employee, reporting certain changes to the Home Office, and ensuring that the individual is complying with the conditions of their visa.

These processes can be time-consuming and costly for the company. They also involve a degree of risk, as the company's Sponsor Licence can be downgraded or removed if they fail to fulfill their duties. Furthermore, visa applications can be refused for a variety of reasons, which can leave the company without the employee they were planning to hire.

Even after all these headaches, there is a 50-50 chance that the government will be convinced to grant permission to that company to hire you. None of the methods is accurate and achievable. Because getting a job in abroad company depends on so many factors such as:

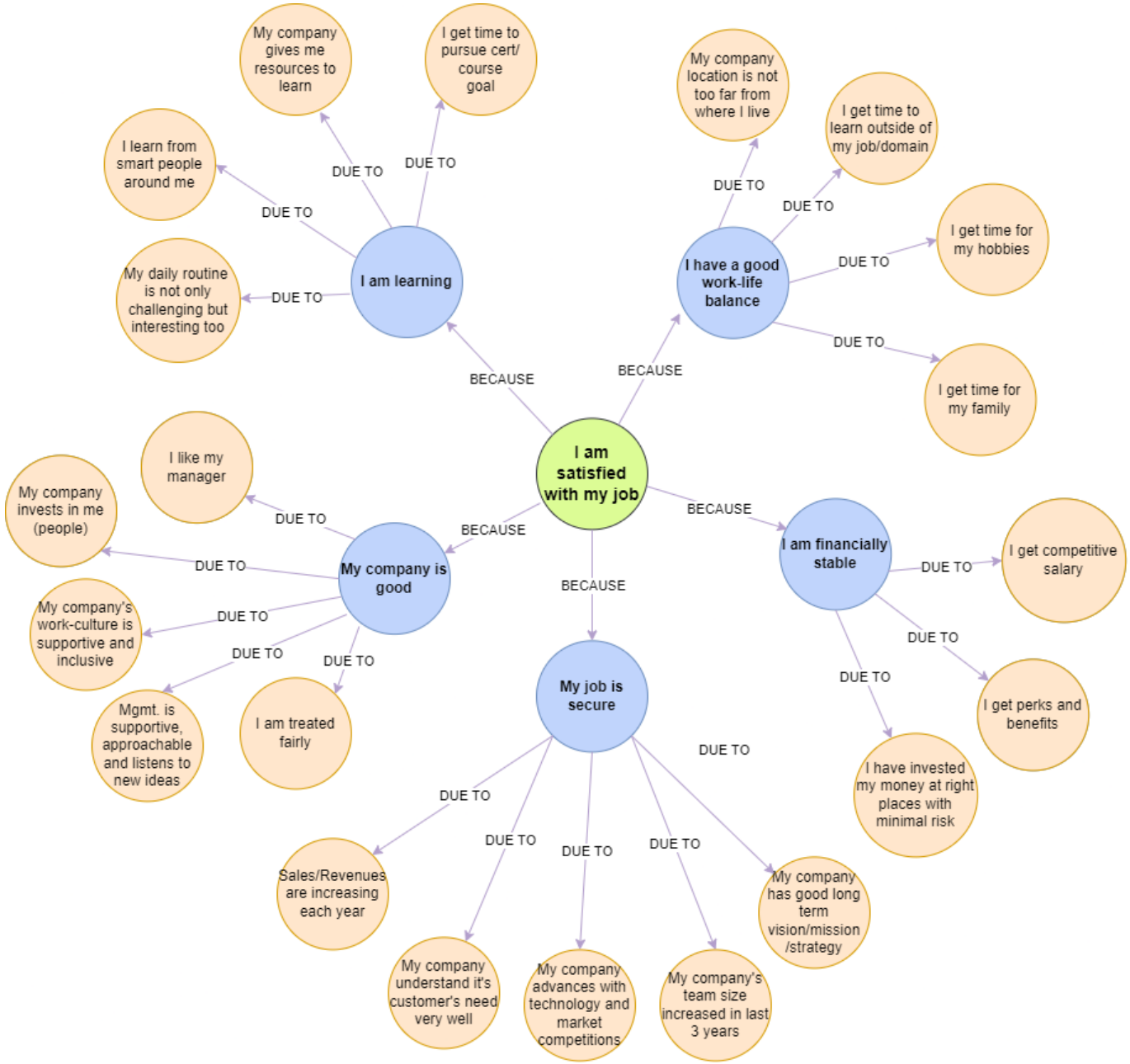
- Target country's strict immigration rules
- If a company is willing to take the headache of visa sponsorship or intend to wait and hire someone locally
- A unique skill set requirement of the job in that company
- Skill shortage in that country, specifically in your field
- Your luck

What is the approach to apply?

Step-by-Step guide you can follow	
Countries	1. Create a list of countries you are interested in working in.
Job titles	2. Create a list of job roles/titles/positions you are interested in or relevant to your area of domains.
LinkedIn Job Filter (Country)	3. Go to LinkedIn jobs. Filter country with one of your dream countries. Give a single job title.
LinkedIn Job Filters (Date)	4. Filter results by latest jobs first through advanced filters of LinkedIn.
Apply for jobs	5. Apply for every single job you think are worth it for you to have.
Create alerts	6. Once you have applied to all the jobs of the last 30 days, create job alerts on LinkedIn for any new job posts that come out in that country. Apply it straightaway.

Change country	7. Repeat the entire process with another country in next week. Keep shuffling countries and repeat the same steps.
Add security people	8. Add 10 cybersecurity practitioners every day in your LinkedIn from the country you want to go in who work in the same area of security as you.
Add security HRs	9. Add 5 cybersecurity HR every day in your LinkedIn from the country you want to go in.
Share knowledge	10. After increasing your network in the local region of your dream country, you need to do create unique, valuable research and start posting regular content on LinkedIn. Let people know who you are, what you can do, what your interests, etc. If they know you more, there are good chances they might want to work with you, or they see you as a potential candidate for their company, etc. *This is important even if you are not looking for a job.*

I am satisfied with my job because:



General DOs and DON'Ts in Cybersecurity

Apart from all the things we have discussed so far, there are still plenty of things you should and shouldn't do in the cybersecurity industry. The following table illustrates DOs and DON'Ts of the cybersecurity industry.

DO
Ask lots and lots of questions to yourself. Such as • Why this way? • Why not that way? • Am I getting investment vs return? • What is my investment (time, money, energy)? • How much investment? • What should I expect out of this? • What if I fail any backup plan? • Will I be only affected by doing this, or will people around me too? • Will I be getting short-term benefits or long term? • Will it give me work-life balance and satisfaction? • Have I reviewed well enough the task, the person in front of me, and the company? • Are there any alternatives?/ Easy way? • How would I measure my success? • Have I checked the accuracy of the result? • What can I do separately to ensure my outcomes are consistent and don't vary, giving me confidence in my work or the goal I am achieving? • Who is my audience? Are my responses tailored to operational, technical, strategic or social audiences?
If you develop more curiosity, you will learn a lot, which is the only way to succeed in our industry.
Keep a target of two years and ask yourself where you want to see yourself in the next two years. Keep achieving this target and then set a new target after two years.
• Share knowledge. Don't just keep it with you. If you share, you will: (Source: https://github.com/s0md3v/be-a-hacker) • Be appreciated and it will motivate you to share more. • Any mistakes or improvements to be made in your content will be pointed out so the overall quality of it will increase. • You can only explain something if you understand it well which can be a self-check to see if you actually know enough about a topic. • Exposure is a great thing. It will bring you opportunities and the power to influence people for good.
It is good to work in different areas of cybersecurity; maybe some of the areas might not be relevant after some years; at that time, if you would have knowledge and skills in other areas of cybersecurity, you would be able to survive and find a new job. It would be easier for you to switch from one domain to another at that time.
Respect gender diversity and give the same amount of respect to all men and women.
Maintain healthy relationships with everyone in cybersecurity because the security industry is very small, and you would meet the same people wherever you go.
DON'T
Do not waste money blindly.
Do not go for the paid courses which are already available freely on the internet

Do not get attracted by fame and money game after bug bounty industry
Do not apply any shortcuts in the industry, whether it's for certification or getting a job.
Try to learn from your seniors but as well as from juniors.
do not defame others
Do not leak sensitive data which are copyright protected.
A rockstar is a person who might be skilled but isn't a very good person to work/talk with. They often have a big ego; they like to work alone because they know* everything and they often look down on people. It doesn't essentially mean that they are bad people because this behaviour can be both intentional and unintentional. The point is, they look bad doing so and more importantly, make others feel bad. To be honest, this is a common problem and I too once started to slip into this zone due to depression, it was not fun, that's why I have included it. Don't be some egoistic genius sitting in a room. (Source: https://github.com/s0md3v/be-a-hacker)

Challenges for beginners

I think below are the challenges beginners face in any industry when they step into the corporate world. Not only I have shared the challenges, but I also shared how you can overcome them.

Area	Challenges	Solution
Communication fear	• Don't understand how to communicate with new professionals in the market. • Don't understand what business and corporate communication vs friendly college/social life communication is • Don't know how to start talking with new professionals • Don't know what to talk what not to talk about until you make a healthy relationship with the new professional	There are plenty of videos on YouTube specifically for business and corporate communication skills improvisation. It is essential to go through it and stand different from your fellow beginners in the market as a beginner. You can use the below keywords to go through YouTube videos. • Professional communication skills • Business communication skills • LinkedIn communication skills • Business communication
Unprofessional communication	Below are some examples of unprofessional communication. • Asking straightaway for reference and jobs • Asking questions for which you can easily get answers from Google • Chasing people often as they might be busy • Writing long intro email until and unless someone asked you • Giving your resume straightaway as you add people • Not checking your tone of the message	Simple, don't do things mentioned in the left column. • Keep patience • Start with simple, small • Build slow healthy relations • Ask experienced people around you to help you • Ask your mentor • Observe how to experience people talk to you when you are talking with them • Adapt different professional people's talking/writing styles to improvise yourself.
Lack of patience	Beginners are very much desperate to get something, whether it's material, an answer to a question, suggestion or even a reply from HR after applying for a job. They send chaser emails, call them, and find ways to communicate with them faster via phone, social media, etc.	Remember, what's essential for you can or cannot be important for others. So, it is wise to keep patience. Keep patience as there are always other ways, different alternatives for your needs. Give them reasonable sufficient time. Don't chase people often as you want things to move desperately.

		Especially for jobs, if HR does not reply after you apply for the job, maybe your resume is not selected. No HR in the world just receives a resume and send it to the dustbin without looking at it.
Writing blunders (Resume, LinkedIn, Email)	Beginners make a lot of mistakes in resumes, LinkedIn profiles and emails to any professional.	I have described all the resumes and LinkedIn blunders in a detailed section of this article.
Lack of industry/corporate understanding	Beginners assume things in their own way, but they are not well-versed with the reality of how corporate works. What you think outside is not the same case as how a company works within the inside. **For example,** submitting 1 bug (vulnerability) to a company, you think why the company has not responded for 4/5 days even as it's just a straightforward bug. What you don't know is, any single bug/vulnerability related comms that come from outside will go through a proper VDP program inside for which app team, infra team, incident management, vulnerability management and SOC team would be a part of. They all are responsible for doing one or many things with that report. Such as: • VM team will communicate that vulnerability to the app team • Infra team will see if an app can be protected by FW/IP based restrictions or not • SOC would see if there were any alerts/incidents or not • App team will fix the bug • VM also checks severity, a risk to business (Risk to business is not only the CVSS you submitted, but what is an actual risk is to business can be only known by the internal blue team) • Management involvement in order to decide how much to pay a researcher • Document all evidence of bug, fix, payment, researcher name, email comms. • Identifying how many similar types of bugs companies know • Checking with traditional vulnerability scanners is why they could not detect those as companies pay for those scanners. • App/Infra/Network team gather and identify the root cause problem business-wide for all similar types of bugs and how they can fix it rather than point fixes. • VM team to identify how they can increase their coverage for those out-of-box vulnerabilities. • Management to ask questions and check in their app pentest/red-team partners why they could not detect the vulnerabilities you submitted. **Another example is submitting your resume to HR of a company and expecting** a response in 5/6 days. Assume if you are the HR of a large company, how many resumes in a day you would get? Also, you are not only filling 1 position but many positions from various divisions of the company. You would be flooded with tons of resumes for all different departments. You will have to go through each one of them, filter them, talk, and discuss CVs with those division leaders in your company, filter candidates, send them emails one by one, keep track of records of emails and candidates, organizing interview rounds, including phase 1 phase 2 and all, aligning candidate's time with the interviewer's free slot, and many other responsibilities. Again, not just for the 1 position you are filling but many in the same company. Hence, when you apply, you should not expect a quick response.	Some tips for you: • Unless and until you work in the industry, you cannot understand how it operates from outside • Don't assume ask around • Keep patience • Keep seeking advice of your mentors
Poor grades	Some beginners will have poor grades in their education, and they are hesitant to show them on their resumes.	You don't need to write grades or show them to any company unless and if they ask you. Just mention what study you have completed. In the cybersecurity world, skills and practical knowledge weigh more than grades. If some companies, ask for grades and also questions you why poor grades you can answer them below:

		• You were interested more in practical knowledge during your education; hence you focused on real skills than theoretical knowledge. • Maybe you might genuinely have some social or other responsibilities or any other reason you got poor grades; you can transparently explain those. • Maybe you are preparing for the cybersecurity certification. So, you don't need to fear even if you have poor grades. You can still transparently show your education stuff on your resume.
Lack of self-learning	I have seen beginners asking many simple questions for which answers are readily available on Google. Self-learning is really required in the cybersecurity industry.	I think the YouTube industry has created so many videos on YouTube which lets you know from very simple things to very complex things; on top of that, you can search all the things easily on Reddit and Google. You should only ask other questions if you cannot find answers easily from Google or any other sources on the internet.
Don't know which companies to go for	Often beginners don't know which company they should apply for a job, whether it's a product base, consulting, or a good security company.	I have covered this challenge & it's solution in-depth within this article.
Feeling demotivation,	there are two types of demotivation. 1. knowledge and skills demotivation 2. Experience demotivation	I have covered both of them in detail within this article, along with the possible solutions.

How to stay up to date with the latest knowledge in the security field

If you Google this, there are plenty of methods to stay up to date in the security field. The best way I found is by using more and more hashtags (#). Individuals and companies both love hashtags. If there are any latest news, people tweet it using hashtags. If you follow any blog, YouTube channel, or any single resource, you will not have other domain knowledge than those creators put out there. If you start visiting many links, you will not be able to keep a bookmark of all URLs, and management would be difficult. All you can do is collection of more and more hashtags.

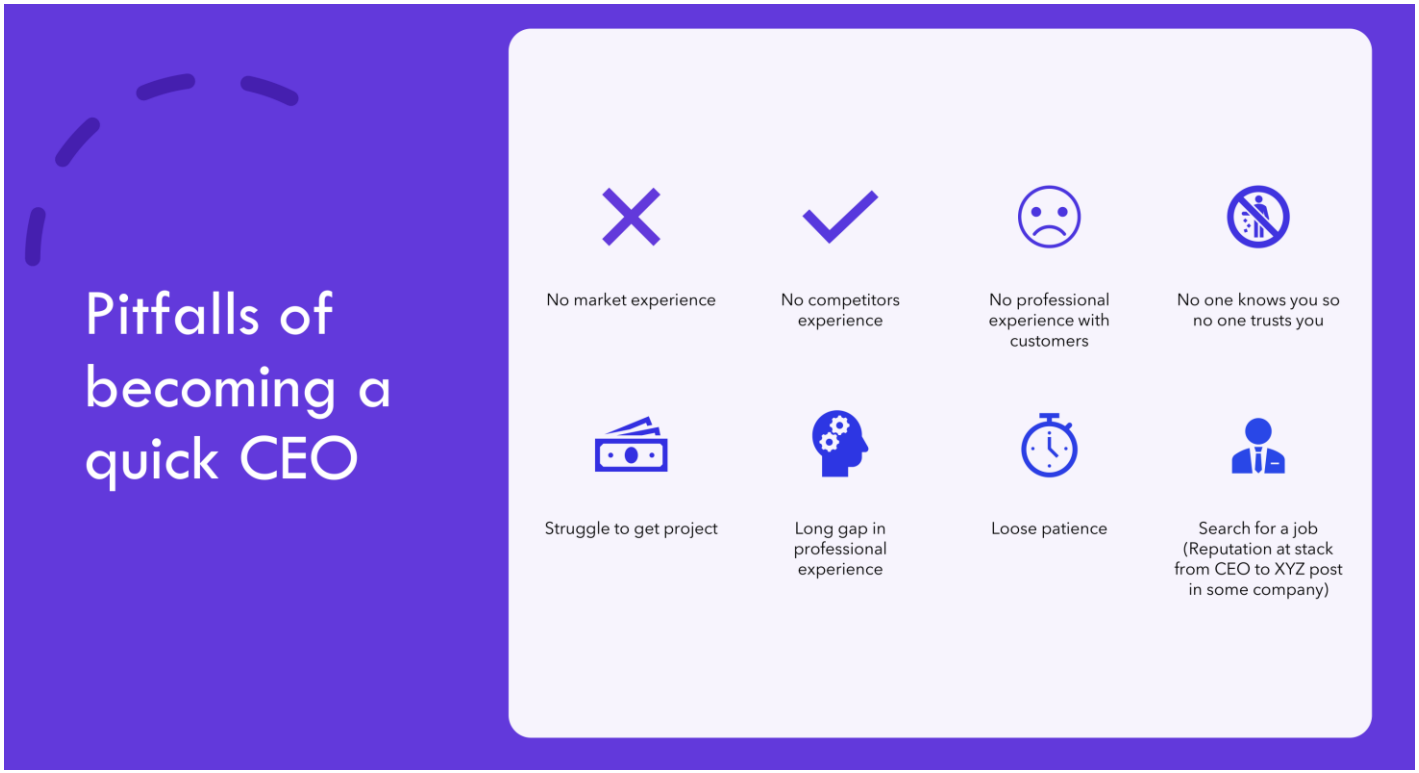
What you need to do:

DO
Know what your area of the domain is specifically (E.g., SOC, Pentest, Cloud Security)
Start listing all possible hashtags in those areas. Ensure you think of a wide variety of stuff while creating hashtags, such as methodologies being used, most common tools being used, other relevant tags being used with that, etc.
Go to Twitter, LinkedIn, search content with those hashtags
Filter noise of data by looking at the latest (last 24 hours, last week) contents only.
Read it
Take notes if required
Repeat the cycle
Create a weekly schedule on reading on 1 topic every day; then follow the cycle.
DON'T

Don't add irrelevant hashtags for which people don't often put any content (simply because they don't use those hashtags even)
Don't add a very long hashtag for which chances of finding content are tiny

Sample hashtag database for you to start with *(you can create your own like this)*	
General security	#cyber #cybersecurity #cyberattack #cyberattacks #cybersécurité #cyberrisk #securitymanagement #securityawareness #securityprofessionals #infosecurity #informationsecurity #infosec #security
Threat intelligence and threat hunting	#threathunting #threatintel #threatintelligence
Penetration testing & security assessment	#pentest #pentesting #penetrationtesting #testing #networksecurity #Redteam
Application security	#bugbounty #bugcrowd #bughunting #appsec #applicationsecurity #apis #webapplicationsecurity #web #webdevelopment #mobileappdevelopment #owasp
Cloud security	#cloudcomputing #cloud #cloudsecurity #aws #azure #gcp

Don't become a CEO/Founder directly without having any corporate experience



Disclaimer - https://github.com/iamthefrogy/Disclaimer-Warning

I have found this scenario that many college/university pass-outs become CEO/Founder/Co-Founder straight after graduation. Some think that having a founder/co-founder/CEO on a profile makes a difference, and it looks cool. I am not saying no one should become an entrepreneur, but my point is without having any proper corporate experience, you should not jump straight into entrepreneurship.

One should not become an entrepreneur in cybersecurity without having any of the **single things** from below:

Solid Product	Unique Service	Solid Funding
When I say solid product means, you created something that is unique and solves a significant amount of problems for an enterprise. There are no products in the market such as you. You have all the features in your product to meet any large enterprise's need.	When I say, unique service means no common services such as pentest, code review, risk management assessment etc. If your approach to providing these services is unique, if you can create a difference and give value to your customers, then it is ok to provide the same services. You need to ensure to provide a great quality of services compared to other competitors in the market. If you are not the one who can make a difference, don't become a CEO at an early age.	Many people might be rich already; if you don't have a great idea or unique service, you can invest your money to create an exceptional service or product with the help of the right mindsets in your team. Even you can invest money into experienced BDMs (Business Development Managers) who already have established contacts in the market who can bring projects for you.

Without any of the single thing from above, there is no way you can survive in the market, and I guarantee you.

Approach to create a solid product:

1. Do a lot of literature review
2. Do a lot of market review
3. Understand what gaps there are in the industry and what kinds of products are not available
4. Evaluate whether you can create something that can fulfil the market's need?
5. How much time/money/efforts would be required for not just making a product but also running its post-build operations
6. How much time it can have to be successful by doing marketing, customers purchase it, and revenue is generated afterwards
7. Which are your target industry and country
8. (A lot of things go in this thought process; these are some really basic before you start)

Post this analysis, create a product, and sell in the market as an entrepreneur.

Since you will be a young, dynamic aspirant, if you go with this all analysis, you will still be excited to work on something as you want to become a CEO, don't rush, the market is very dynamic, almost there are every solution in the market, and they are good even. So do proper research else, don't even think about this.

I have seen plenty of people who started their company without having any of the above and then:

- Not able to serve client properly as they don't understand how big corporate works internally
- Not able to beat their competitors as they don't know what they are up against
- Not able to know how the market industry works as no experience of working in corporate at all
- Struggle to get a project as they don't have good funding to invest, unique service or unique product.
- No one knows about you as you are an absolute fresher with no credible experience or achievements.
- You lose patience after a few years of trying to run your company, and when you close it, search for a good job with a stable income in any big company.

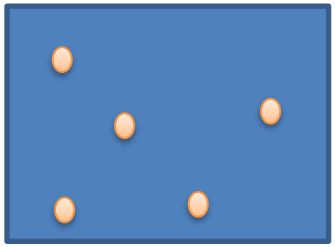
How not get demotivated in cybersecurity?

Demotivation in cybersecurity is not a new thing. Due to the high amount of competition in security, things such as attitude, knowledge monopoly, marketing of experience and knowledge is common. A lot of youngsters who get demotivated when:

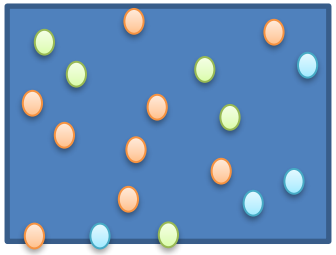
- They see other's success
- They are not treated well by others (in or outside of the company)
- They can't find a way to get success
- They see money and fame games on all social media about bug-bounty and other stuff
- Any other reason…

What you really need to know is this:

Knowledge/Skills Demotivation



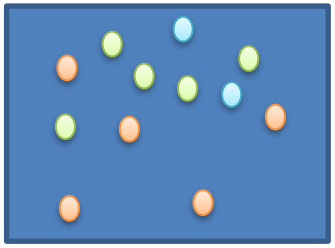
You know

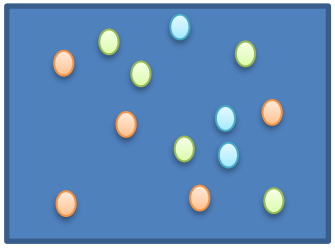


They know

You learn

Now





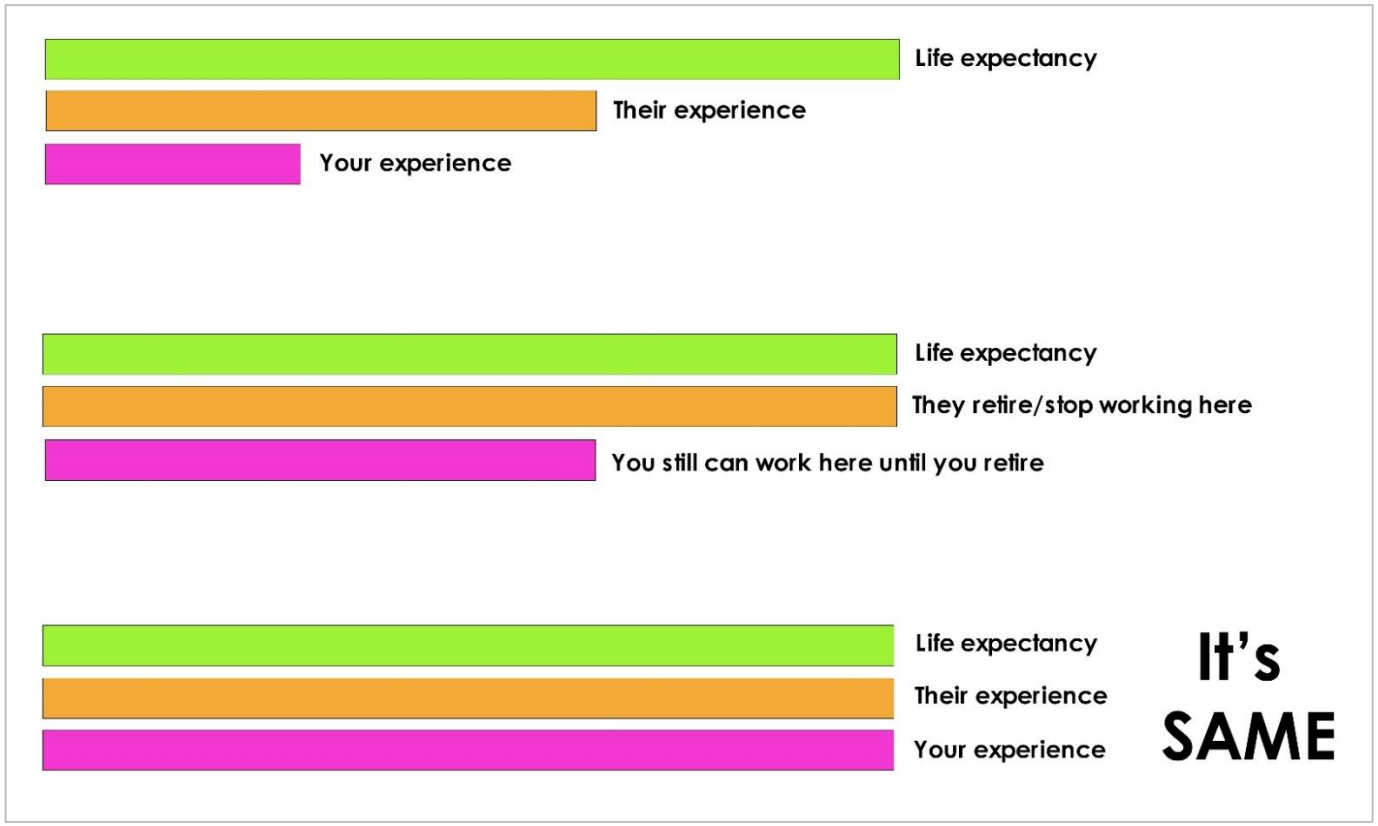
You know SAME as They know

You need to take this as a positive approach and keep constant learning without getting demotivated. If another person knows 5 things, you learn them from YouTube, Blogs, Courses, and Free materials. Now you and they both have the same knowledge, so there is no need to get demotivated in security if you don't know things.

Be grateful that you met that person through whom you came to know what else you needed to learn. Make a not, learn it. Have the same knowledge as they now. Mission accomplished.

Experience Demotivation

If you get demotivated by someone's massive experience in cybersecurity, always believe in the below diagram 😊



So at the end we all are same. In fact younger generation (pink bar) has slight advantage in this case where they can learn new technology and advance their last couple of years of career when older generation (orange bar) has already retired by that time.

Appendix 1 - IT to Cyber domain/role mapping

It is not a 100% mapping of all IT roles to all Cyber, just a heads-up.

Network Engineer, Network Administrator, Network Architect
Network security
Firewall, IDS, IPS proxy
Filtering
VPN
DDOS protection
CIS benchmarks for networking devices
Infrastructure VAPT
Security Log management and analysis
DevOps, Web Developer, Software Developer, Development Manager, Project Development Manager (Agile/Scrum Master), Project Manager, Database Administrator, Database Engineer, Quality Tester, QA Engineer
Threat modelling
DevSecOps
Design review
Secure coding
Static Analysis
Bug bounty
VAPT
Application security testing (Web, Android, iOS, thick/thin client app testing)
SAST
DAST
WAF
RASP
CIS benchmarks for anything in application security

Windows Administrator, Server Administrator, Linux Administrator, System Administrator, Windows/Linux Engineer, IT analyst, IT Helpdesk Analyst, Helpdesk Technician, Technical Support Engineer/Specialist, Programmer
Endpoint security
Anti-virus/anti-malware
EDR solutions
HIDS/HIPS
App whitelisting
Patch and Image management
Vulnerability and patch management
Infrastructure VAPT
Secure configurations
CIS benchmarks for OS
Auditor, Reviewer, Compliance Manager, Financial Auditor/Reviewer, Legal and Regulatory and any Senior Leadership within IT role
Compliance (PCI, SOX, HIPPA, NIST, FedRAMP)
Privacy and GDPR
ISO, SOC1, and SOC2 audit and review
Lawsuit Risk
Risk management
Security strategies
Identity and access management
Business impact analysis
Vulnerability Management
Risk assessment
Security awareness
Vendor risk management
DR/BRP
Policies, Procedures, Frameworks

Cloud Architect, Cloud Consultant, Cloud Service Developer, Cloud Administrator, Cloud System Engineer
Cloud infrastructure security
Cloud penetration testing
Cloud security architect
Cloud security monitoring and detection
Cloud automation in DevSecOps
Containers & Kubernetes security
Incident Manager, Incident Handler, Investigation Specialist/Officer, Crisis Management
Incident response
Breach investigation
Forensics analysis
Breach communication
Crisis Management
All DevOps roles in Cryptocurrency & Blockchain Industry
Blockchain Security
Assembly Programmer, Assembly Technician/Specialist
Malware analysis
Reverse Engineering

References:

- https://www.careeraddict.com/choose-master-degree