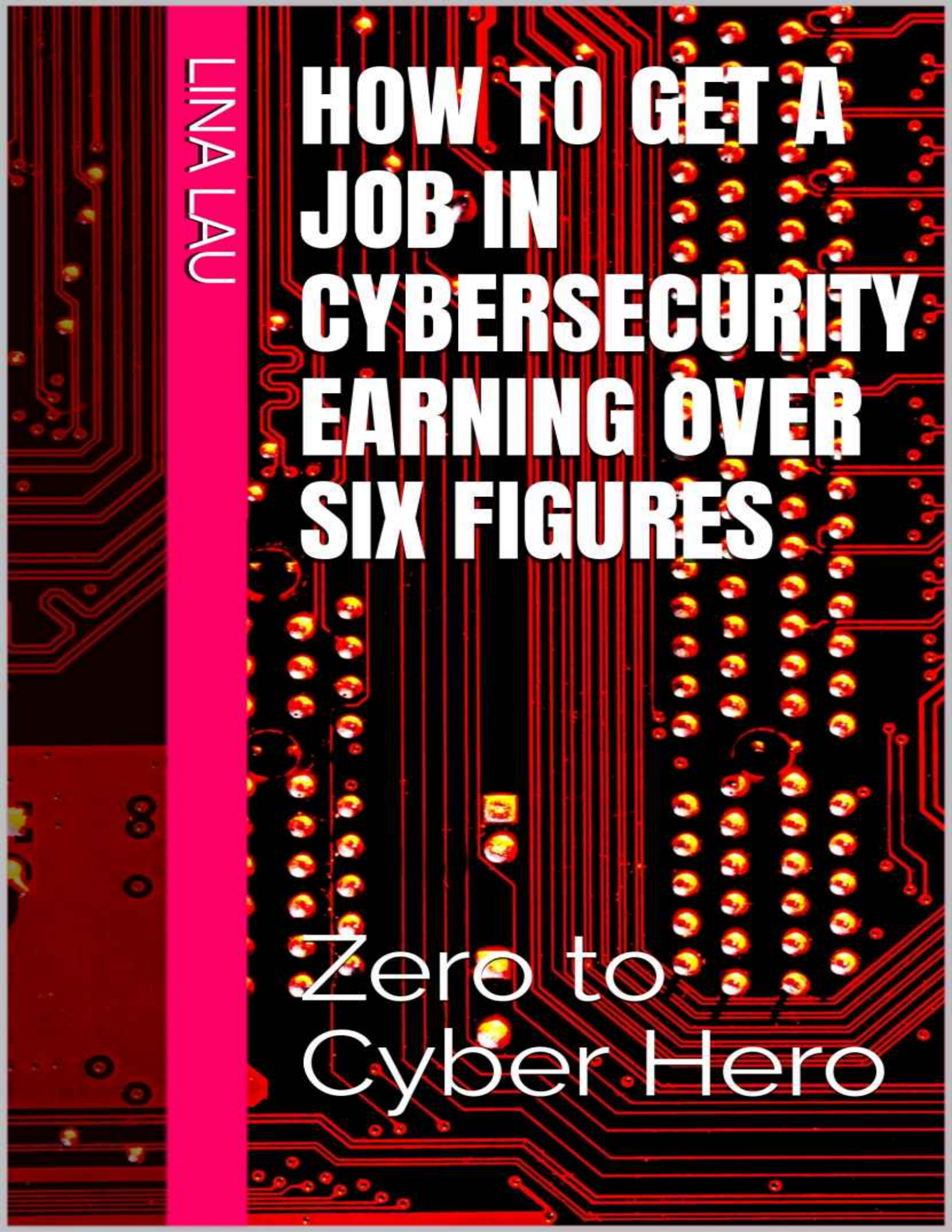

LINA LAU
HOW TO GET A JOB IN CYBERSECURITY EARNING OVER SIX FIGURES
Zero to Cyber Hero

Table of Contents

Step 6: Mindset and principles to remember

Onwards and upwards

Introduction

If you are seeking a job in cyber security but don't know where to begin, you are in the right place. Your motivation may rise from something you saw on TV or a movie, an interesting news headline, gotten a taste at hacking on something, or are simply fresh out of school and are looking to break into the field. If you want to take this motivation and turn it into a career, this book is intended to be a helpful foundation for that next step.

I was in your position once. I fell in love with malware, wanted to work in the field and I had no idea how to get my foot in the door. I would read cybersecurity Twitter feeds and not understand basic things like what a CVE was. There was a lot of self-doubt and I questioned if I was 'good enough' or 'qualified enough' to get into the field. I dropped out of University and that only intensified my anxiety about if I was 'good enough'. There was one thing I did know. I couldn't get into cybersecurity following the normal route of 'getting a degree', competing with thousands of others trying to land an entry job with '3 years minimum requirement' written on it. I wanted to accelerate my career trajectory, and this book is about how I did this. I hope it helps you with some principles you can apply to fast track your career and excel in this field.

I am not the type of person who would ever write a book as it is just not something I enjoy doing. But I noticed on LinkedIn a lot of graduates and people asking for advice on how to break into the field and I saw a lot of terrible advice from recruiters and a few senior executives. Their advice ranged from 'keep trying' to 'apply anyway'; hardly meaningful feedback. In principle, they are right, but in practice this 'don't give up' advice is useless when you have not built the right foundation on which to excel in this field.

The road is long and will require hard work and determination. There is no short-cut to gaining knowledge. As much as I wish I could download peoples' brains, I can't. The purpose of this book is to teach you *how to fast track your career,* but you still need to put in the work. There is no 'fast track success' pill that will make you rich or successful and if someone is selling you that, they are scamming you.

This book covers how I got into cybersecurity. You may not have had direct work experience, specific skills or tooling experience, but the methods I will cover might help you overcome your 'on paper' limitations.

You will learn:

- Average salary expectations and benchmarks
- Common recruiting lies
- The negative side of each job in cybersecurity
- Building a network and reputation
- Resume and social media tips
- Acing the job interview
- Technical and practical interview tips
- Dealing with prejudice and judgement

The knowledge in this book is based on my experience, my opinion and the opinions of those in my security network. This may not represent the viewpoint or experiences of everybody.

Step 1: Define what you want to do

It will be harder for you to get a job in security if you have no idea what you

want to do. How can people help you when you don't even know what you want? You have two options – either apply for a rotational internship program with consulting companies / banks or, read on and try and figure this out for yourself.

Cybersecurity is a broad term. There are several niches and various roles you can fill in cybersecurity – each with positives, and negatives. There is no such thing as a perfect job. You will always face struggles, for example… work-place stress, politics, confused clients, unrealistic deadlines and hours of Microsoft Office i.e. Excel, Word, PowerPoint. (No offence if you really enjoy using Microsoft Office).

In step 1, I will cover what each of these roles are – what skills are needed for them, how much they pay, and some lessons learned from each role. These are the kind of thing that they never write on the job descriptions. For each of these roles, I have spoken to colleagues and friends in each of these roles and gotten their honest opinion.

Do not read this and start looking at job advertisements that say, "3 years minimum experience" and feel disheartened. These job advertisements honestly don't mean too much if you have the skills and can show you have the same equivalent knowledge for it in a tangible way – unless you're being interviewed by someone who is very narrow minded. In that case, consider how much you'd learn being managed by them. When I come across people like this, I see it as a red flag and run. Just remember, 3 years' experience does not mean someone was learning for that entire 3 years. I have interviewed people with 10 years' experience and did not have that much to show for it.

The Difference Between IT and Cybersecurity

Even though IT and cybersecurity have several crossovers, there are several intrinsic differences between these roles. IT roles often focus on infrastructure – the setting up of systems used by a company, or the management of such systems. They may also focus on networking and managing the network of a company. IT based roles also encompass architecture roles where an architect might be asked to design how the infrastructure works for a company and what tools are used.

The difference between IT and cybersecurity is that IT focuses on the systems that are used, setup and managed and security is all focused on the security of these systems and various security tools.

This guide does not cover anything about IT roles or how to get a job in IT. However, a grounding in an aspect of IT – networking, scripting, server administration, cloud administration or otherwise, can be seen as a real asset to someone's skills. Just because you have spent your career configuring switches or changing passwords, your skills are just as applicable. If you have a strong knowledge about active directory, there are several security companies hungry to hire you. Make this known.

Consulting or an Internal Team?

If you don't know what this topic even means – let me take a step back. There is a timeless debate between whether or not people should move from a consulting company to an internal team. Simply this means, do you want to work in security managing the security of the company you work for (i.e. if you work at Lauren's Technology Shop, you would manage the security of Lauren's Technology Shop) or if you want to join consulting and manage the security of several different companies.

There are pros and cons to each. Working in consulting can be stressful and you need to be comfortable speaking with people, running meetings and presenting. Each client has different needs and requirements and will be different to deal with. You will constantly be faced with different security environments and be faced with things you do not know. Consulting also means you might be surrounded by different people all the time depending on how long each project lasts for. If you thrive in a dynamic work environment and want different challenges and a different environment every day, then perhaps consulting will interest you.

Working for an internal team means you are working with the same internal core team and managing the security of that specific company. Sometimes it pays better than consulting (depending on how well the consulting company you work for pays). Internal teams provide more structure and more consistency and can sometimes be less stressful than consulting if you need stability in your working environment. With that said, I have seen people work for an internal team and be heavily stressed just the same as in consulting.

Cybersecurity Roles

The table below summarises the types of roles that fall under cybersecurity and what they broadly consist of. Please keep in mind that the roles companies come up with often vary due to what lexicon they choose to use. I have even seen some start-ups name their roles “Cyber Unicorn” and go on to describe the role of a cybersecurity analyst. If you ever feel confusion with a role, it’s best to read the role description and speak with the HR manager to get an idea of what the day-to-day life of that role is.

Note: This does not include any cybersecurity roles pertaining to project

management or sales related cybersecurity roles.

Job Area	**Advertised Job Role**	**Broad Description**
Offensive Security	Junior/ Senior Penetration Tester Red Teamer Product Tester Social Engineer Physical Security Tester	Technical role focused on breaking into computer systems, products, physical systems / buildings to test for vulnerabilities. This role is often thought of colloquially as a “hacker” or a “white hacker”.
Threat Detection (Security Operations Centre or Network Operations Centre)	Threat Detection Analyst SOC Analyst NOC Analyst Detection Analyst Detection Engineer Cyber Operations Analyst	Threat detection-based roles are often focused on trying to detect cyber threats against a resource, product, network or endpoints. Some of these roles will include some basic triage and response efforts to cyber incidents.
Security Engineer	Junior/Senior Security Engineer	Engineer based roles are often focused on configuring, building or developing systems used by the security team

Threat Hunting	Threat Hunter	Proactively looks through the network to try and find any threats that have escaped detection.
Incident Response	Junior/Senior Incident Responder	Technical role focused on responding to breaches or intrusions that cannot be handled by the Threat Detection teams. This role includes investigating the breach and determining the root cause.
Risk and Compliance	Cybersecurity Consultant Cyber Risk Consultant, Risk Analyst Compliance Officer Exposure Analyst	Performs written assessments of how much risk a company, process, data or product is exposed to.
Malware Analysis	Malware Analyst Reverse Engineer	Technical role focussed on disassembling malware, analysing malware origins and determining what a piece of malware/software does.
Threat Intelligence	Threat Intel Analyst Threat Officer	Focused on tracking various threat groups in both nation state

		(government sponsored) and also commodity groups (organised crime). This role often focuses on collecting data that helps security teams identify who is attacking them.
Security Researcher	Security Researcher	Conducts research into various security flaws, security products, tools, and vulnerabilities. Researchers can also work on developing new tools or finding zero days that can be leveraged by a penetration tester.
Cybersecurity Analyst / Consultant	Cybersecurity Analyst Cybersecurity Consultant Cyber Leader Cyber Program Manager Cyber Practice Lead Cyber Awareness Lead Cybersecurity Specialist	Broad umbrella role that is used to cover a wide range of focuses. Consultants and analysts often perform a myriad of functions across threat detection, risk, report writing, documentation, liaising with clients, offensive security work and also blue teamwork. Reading these job descriptions should give you a better indication of

	Cybersecurity Advisor	what is involved in this job.
Upper Management Roles	CISO CIO CTO	These are management and vision focused roles. These are decision-making roles used to address the technological improvement of a company, what products they should use and how the security teams and functions should be set up for maximum effectiveness.

Salary Expectations

The table below summarises a broad estimation of how much these roles pay. Please keep in mind that some companies may pay more or less than what is included in this table depending on their financial situation and how much they invest in their security teams. Further, some security professionals do not want to join management and would rather stay in a technical role. For these individuals who have remained in their technical role for +10 years, their salaries will be well over what is included in this table. This table is just to serve as an average estimate of how much these roles pay.

This table is a product of my personal experience, the experience of my colleagues and security network and also as a product of conversations with several HR hiring managers for the cybersecurity industry.

All figures shown below are in USD.

Job Area	Salary Band (Junior – Senior)
Offensive Security	$80,000 - $200,000 +
Threat Detection (Security Operations Centre or Network Operations Centre)	$50,000 - $120,000
Security Engineer	$100,000 - $160,000 +
Threat Hunting	$70,000 - $90,000
Incident Response	$80,000 - $200,000 +
Risk and Compliance	$40,000 - $150,000 +
Malware Analysis	$80,000 - $200,000 +
Threat Intelligence	$50,000 - $170,000 +
Security Researcher	$20,000 - $200,000 +
Cybersecurity Analyst / Consultant	$40,000 - $200,000 +
Upper Management Roles	$300,000 +

You may notice that there is a wide band for each of these. It is not uncommon to see certain roles fetch $250,000 +, but there a number of factors that go into how an individual can achieve these salary figures. These factors will be covered in the rest of the eBook as we will go on to discuss how you can land a six-figure role as a graduate or a drop-out with no prior experience.

Good Bad and Ugly

Often when you interview for a role, the hiring managers or the recruitment agencies do not give enough detail in the job descriptions to give you an

accurate representation of the role. Their role is to attract interest for the role and provide the initial screening. This makes it your job to ask the right questions and determine if this is the right fit for you. This means, people who are new to the industry and don't know what to expect often find themselves sold into a version of a role that does not reflect what was sold to them in the initial interview stages. There are organisations and people that will prey on the 'greenness' of someone and their 'eagerness' to work. A lot of newcomers have this 'I will do anything' mentality and will often be overworked and underpaid. Just watch out for this because working 'more' does not mean you will be 'paid more' or 'respected'. There are more effective ways to approach this situation.

A common tactic used in recruiting is to outline what is 'exciting' about the role and what you can expect. The anecdotes that they pass commonly only describes instances of what you would be doing based on the "best day" versus the reality of the "everyday". To avoid turning away highly sought over candidates, the hiring managers often do not stress how much of the "boring" or "ugly" side of the job exists. For example, someone in an interview might tell you in a penetration testing role something like 'our penetration testers hack into vehicles and have found multiple zero days'. If you are a junior this is most likely not going to be you. What this means is you will most likely be working on junior cases and those 'cool' car hacking cases are done by the elite team within the organisation. Unless you are talented, gifted and do all the right things (which no offence does not happen often) you are looking at years before you hit that point. But with this, if there is something you really enjoy in your job or have a real aptitude for, please make it known. You might find yourself becoming a specialist in something in no time!

It's important when you read the job description and when you speak with the job manager that you ask some important questions – such as always asking the division of time dedicated to what tasks. For example, when told

by a hiring manager that you will be working on detecting threats and dealing with alerts and some reporting – you should always ask questions like how much percentage wise of my time would I be working on X versus Y. Ask for the best case scenario of this and also the worst case scenario.

Another critical question that I think is important to always ask in a job interview is the churn rate of staff. How often do staff quit – and what are the primary reasons leading to them leaving. High churn rates often signify employee dissatisfaction, high stress environment, toxic culture, bad management, underpaid staff and or lack of fulfillment at work. Again, I will be covering more about applying for jobs, resumes and interview tips in the later parts of the eBook.

This next section delves deeper into the main pros and cons of working in each field.

Offensive Security

Penetration testing, red teaming or adversarial type simulation roles focus on breaking or 'hacking' into a system, person, product or physical building/infrastructure. These jobs are often time-boxed and used by companies to pass a compliance test or to test the security measures they have put in place to prevent future intrusions.

The role of someone in offensive security means you constantly need to be refining your skills, learning new methods of breaking in, learning how to hide your tracks from security tools, learning social engineering tricks and also refining your methodology.

Lessons from the job

- *Repetitive work – when you first join you think you will be constantly breaking into 'cool' systems but there are aspects of the job that bring consistent revenue to the company like pen testing APIs or web apps that can become repetitive*

- *Half of the job is spent writing reports. You have not finished your penetration test or red team until you have written a report that contains all findings. This means you spend half of your time typing on the keyboard and it's very boring.*

- *High stress environment because you need to break into a system with a given time constraint and sometimes due to skill, time or lack of technical know-how or tools you can't break in.*

- *You need to be sensitive to how a client is feeling. Although you are ecstatic you broke in, often the client is not happy about it because it means there is some vulnerability or flaw in their system.*

- *The constraints placed around penetration testing often does not mirror real life. There are often "no-go" zones and it's a highly simulated environment that does not reflect hacking in real life.*

- *Weird cultural pressure where everyone competes with each other about who knows more about what. This might differ from company to company, but often people are looked down on for being "bad" and there is a certain level of gatekeeping in this field.*

Threat Detection

Detection based roles form part of the blue team in a cybersecurity field. These roles centre on detecting threats or cyber-attacks targeted at the

organisation that you work for. The typical day-to-day life includes looking at a list of alerts that you get and starting the initial investigation and if it gets to a stage where it becomes too difficult, or the threat is too great – then these incidents would be passed over to the incident response team. The threat detection-based roles may also include some level of methodology development, playbook writing or working with specific cybersecurity tools. The most common tool that a threat detection team would use is typically a SIEM – a security incident event management tool where all of the logs and events from an organisation are pulled into a centralised platform. Based on the alerting criteria that a detection analyst might write; these would trigger alerts which may or not may not require analysis and investigation.

People working in threat detection stay at the front line of all cyber-attacks as they are the first filter for everything that occurs. This requires people who are in this position to stay up to date with the latest cyber threats, vulnerabilities and TTPs (tactics, techniques and procedures) that threat actors use to attack organisations or people.

Lessons from the job

- *Repetitive work – you may get several alerts every single day for the same kind of event – for example, an increase or spike in network activity. These still require investigation and a close-out of the investigation. This can become very repetitive over time.*

- *A lot of writing. Every time you have an alert, you need to follow a playbook, investigate what has occurred but you also need to document everything that you have done and your findings.*

- *Overwhelming because there is usually a high level of alert fatigue. There will always be security systems setting off alerts as it's normal*

for constant activity to be occurring outside and within the network. There will be an endless amount of alerts every single day waiting for you to close off and investigate.

- *Frustrating to work in this role when most of the threats are false positives. This means a lot of time is spent investigating something just to rule out that it was a new implemented tool, or some user error.*

- *Sometimes it feels like the work is useless because there are predefined playbooks telling you how to investigate. You don't get to use your brain that much and it becomes extremely monotonous.*

- *It's hard to break out of threat detection and move into a more senior role doing something else.*

Security Engineer

Security engineers often focus on the building of systems or tools that are used by the security team. For example, if a security operation centre (SOC) wants to use a new SIEM tool, the security engineers would be working to ensure that this SIEM tool is working correctly and has the right forwarding rules set up to pull the events into the tool. Security engineers would also be troubleshooting tools when they don't work or figuring out ways to help do things at scale. For example, if an incident responder requires 30 disk images to be taken and stored somewhere – it would be the security engineer's job to figure out the best way the systems can support this kind of work.

The day-to-day life of a security engineer mainly focuses on troubleshooting problems, writing scripts to solve smaller issues or general maintenance.

There is usually a large security transformation project going on and the security engineers would need to work with the IT teams to figure out the best way to engineer the systems to deliver the results.

Lessons from the job

- *Lack of control over what we build and do. Upper management often choose what we need to deploy, or we listen to how other teams want to build their tools. We do not have control over the design and functionality as much as we want to. This is frustrating if that is a reason you are choosing to work in security engineering. For you to reach some level of control you need to be higher ranking.*

- *When you join a security team where things have not been set up properly, you are dealing with systems that are inherently broken at the core. It is not possible to engineer fixes to things that are fundamentally broken. This impacts all the decisions that you make regarding how to build or set-up other systems.*

- *Larger companies like to hire people who are specialists in engineering a certain type of tool. This means it's harder for a team to work together to figure out how systems talk to each other as each specialist is only a specialist in their tool. This creates a lot of team friction and frustration.*

- *High amount of stress. When things break and people complain it's hard for you to not take things personally.*

- *You need to adapt constantly. There might be a new tool or something that the team is building and working on that you don't know what it*

is and how it works. You need to be comfortable learning on your feet.

Threat Hunting

Threat hunters are people who typically work closely or sometimes within a threat detection team. These people focus on proactively and iteratively searching through the logs, events and systems for evidence of compromise. They generate hypotheses based on their knowledge of the architecture and network of how the environment would best be compromised based on known attack frameworks – and they use these to guide what they "hunt" for in the environment.

When threat hunts find signs of malicious activity, or weaknesses in the network, these are directly used to trigger an investigation by the incident response team / blue team based on the severity of the threat. For any findings or logging gaps that occur in a company, these are fed over also to the threat detection / SOC teams and also to the security engineers for them to fix or prioritise whether or not it's important to be fixed. If threat hunters find something that the detection team has not seen, this is directly fed into the threat detection team to refine their alerting rules and criteria.

Lessons from the job

- *Gets very repetitive and you run out of ideas to hypothesize. There's only a number of Mitre Att&ck techniques that exist. Imagine sitting and hunting for the same things over and over again. It becomes very boring – especially when most of the time you do not find evidence of it because those things have already been caught by alerts.*

- *You rarely find something novel and "cool". Most of your findings will be something like unwanted software installations like "utorrent"*

or random browser extensions or programs people decide to download onto their laptop. This is not very exciting.

- *If your threat hunting team is mature, then there is a set methodology that can be deployed every time you are threat hunting. If your security team is mature, then most of the hypotheses you have or things you are looking for should already be automated and built into a dashboard. This makes the job easier.*

- *Working in consulting, often clients do not have the data you need to properly hunt and look for things. This is very frustrating because you do not feel like you are doing your job properly. Even when you deploy an EDR tool (endpoint detection and response) this only collects telemetry from the deployment point going forwards, never historical data. This means you're hunting for things that might be showing signs of badness just in the time period that you're hunting and if something occurred prior, you may not catch it.*

Incident Response

Incident responders are people who handle critical/severe security incidents that occur. These can range anywhere from business email compromises over to nation-state sponsored threat activity (i.e. Russia hacking the company you work for). The role of an incident responder focuses on working out the root cause, how they got in, who did it and what did they do / if they stole anything. Often these incidents go on for weeks, sometimes up to 6 months or more. The findings from these incidents are reflected in recommendations that responders make to organisations regarding how to future-proof or improve their security to prevent the same incident occurring again.

Incident responders have skills in digital forensics and should already possess all the information and knowledge that threat detection teams and threat hunters have. To be an effective incident responder, you also need a level of knowledge that covers how systems are engineered and how they interact.

Lessons from the job

- *High stress. Get ready to be called on Friday night at 5pm for an incident that requires work over the weekend and 24/7 support. Mature organisations will have teams around the world that can handle the overnight shifts – but smaller teams and organisations will not, and this means you might be on call for the weekend.*

- *High pressure. You are working with clients or your internal team under high pressure. In most security incidents the organisation is losing money and might face data breach laws. This means people demand answers from you and want the incident dealt with and fixed in the fastest time possible. This is not always possible because it takes time to investigate systems.*

- *Awkwardness because sometimes these threats are "internal" people who are trying to steal information, data or money from the company they work for. This means often during an incident; people may be fired. This is an awkward circumstance especially when you know them and find evidence that they are the ones that were involved.*

- *There is a lot of pressure to get things right. If you do not figure out how things happened this might occur again.*

- *The best case is that all the data is there on the systems and you have all the data you need to investigate and work out what's happening. The reality is organisations are multifaceted with several third parties. In almost 95% of the cases, a lot of the data does not exist because either there is no logging set up or the third-party IT provider decided to wipe the drives because they are too busy focused on remediating.*

- *Smaller companies do not understand why incident response is necessary and they often ignore advice and focus straight on remediation and making sure business is back to usual. This blows away a lot of critical evidence.*

- *Get ready to see clients who may ignore your advice get hacked over and over again.*

Risk and Compliance

People who work in risk and compliance focus on assessing the amount of risk companies are exposed to. This is used to inform business decisions, organisational changes to security or IT systems, the purchase of new tools/systems and also auditing obligations. The role of someone working in risk and compliance is very focused on using industry standards in building risk matrices and criteria for assessing the "risk exposure".

Lessons from the job

- *If you have a talent for writing or coming up with reasons why something is risky or something is not, this is the perfect job for you. There is a lot of writing and excel/word documents involved.*

- *Most of the risk and compliance frameworks focus on trying to make objective risk judgments. At the end of the day this is not always possible because half of the time even with these criteria, the way you rate it is still somewhat subjective.*

- *A lot of the times when you assess the risk of something, it is something very trivial like for example, should this tool change this configuration. It is not always some ground-breaking change or tool that the organisation wants to push.*
- *You will become a master with the Microsoft Office tool suite.*

- *There is a lot of hate on risk-based roles because it's not seen as sexy as the other roles. But at the end of the day it is necessary to help inform decisions and to make sure the due diligence is done before all decisions made. For start-ups and smaller companies, this may be red tape.*

Malware Analysis

Malware analysis related roles focus on dissecting and analyse malicious indicators of compromise such as an executable, binary, IP address or library. This role focuses heavily on being able to set-up a sandboxed environment and having skills to statically analyse the malware sample and also dynamically analyse the malware sample. To do this, this requires a blend of both the ability to know what 'normal behaviour' is and what is malicious behaviour on a computer system. Static analysis requires skills in assembly and being able to dissect code and reverse engineer the sample to determine what it is doing.

The analysis output from malware analysis is used to inform security teams

about what the malware is supposed/designed to do and also what changes it makes on the system. Malware analysis is also used to help determine attribution of where this piece of malware comes from – i.e., is this a piece of malware written by the Russian government or is this a remote access tool written by a 12-year-old and sold on the dark web.

Lessons from the job

- *Make sure you know how to document your findings in a way that is understandable by everyone else otherwise your analysis is pointless. The job is to help inform incident responders or threat intelligence teams what the sample is and if you give them the data without explaining the implication, it's almost useless and makes their job harder. For example, if the sample makes an API call to a native windows API, and that API is used in process hollowing – this needs to be explained to the team that asked for the analysis.*

- *You will always be learning. There is so much depth in this field and it goes deeper and deeper. The more you learn the less you know.*

- *Sometimes it is very boring when you are analysing things that have been given to you by a security team and it's a sample that is not malicious or a very simple sample.*

- *Get ready to bash your head in because you will face samples that are hard to dissect and you will waste a lot of time chasing down things that you think are 'interesting' but lead nowhere. Often these analyses are timeboxed and quite often, based on how much cloaking actors do this makes your job harder and take longer – which is their exact purpose.*

Threat Intelligence

Threat intelligence roles focus on providing insight to security teams about who the threat actors are that might target your organisation, how they attack you and what they are trying to achieve. Threat intelligence teams focus on tracking, tracing and keeping up to date with the threat actors' and the infrastructure they use. Threat intelligence teams are utilised by the blue team and also the response team to feed indicators like "IPs" or behavioural indicator such as "phishing" to help track, identify and perform attribution on who is performing the attack.

After incident responses are performed, the data that is collected from the incidents are often given back to the threat intelligence teams so they can track and keep up to date with the latest infrastructure or techniques a particular group is using. Threat intelligence is also used to help inform threat detection teams about what the most important threats are and the kinds of alerts that need to be written to help identify the advent of these threats.

Lessons from the job

- *Indicators often go sour. Threat actors share infrastructure so a lot of the times the collected IPs or other indicators become disassociated with the threat actor as they swap from infrastructure to infrastructure. This means that the threat intelligence you are providing can become dated.*

- *Sometimes I feel like a manual ingestion machine because all I am doing is pulling threat intelligence from open sources, closed paid sources and incident response teams and putting it into a tool.*

- *It's rewarding to be able to know a threat group or a threat actor back to front. The more you learn about how they work and what they do, the more you're able to be informed about why they use a certain tool or choose to stay hidden for a certain amount of time in the network.*

- *Attribution is difficult because sometimes threat actors pretend to be other threat actors and if you don't have enough supporting evidence, it becomes difficult to work out who is what.*

- *I am writing reports every single day. I spend almost my whole day writing reports.*

Security Researcher

The nature of a security researcher role can vary based on what the company is looking for. There are security researcher roles focused on android-based malware, security researcher roles looking for people who can find zero-days and other security researcher roles based on trying to identify flaws in an operating system.

The nature of the role is highly research focused, but most of the time the people hiring researchers want a tangible output that is applicable to the security systems today (not a theoretical exercise). There are security researcher roles that work in tandem with penetration testers that focus on trying to identify exploits that can be then utilised by the penetration testers on their engagements.

Lessons from the job

- *This job is not for someone who is not passionate about the area you are researching. For most people to get a role in security research you often need some level of proven expertise in the field and most of the areas are niche.*

- *There are not a lot of security research jobs on the market as not a lot of companies have a need or financial ability to pay for someone who is heavily specialised in one area.*

- *You probably will not have control over what you are researching as what you are researching typically needs to have some direct contribution to the bottom line for the organisation that is hiring you. The only difference is you will be the one dictating how you conduct the research.*

- *When you do research, you need to spend time documenting your research and what you have found and be able to communicate the implications of your research in a higher level.*

Cybersecurity Analyst / Consultant

Cybersecurity analyst or consultant roles tend to be a blanket term that is used across many organisations and can mean many different things. For example, in the large consulting firms an ‘analyst’ or ‘consultant’ role can be mean someone who does a little bit of everything, or it can also mean a risk analyst or a penetration testing analyst. All of this differs across organisations and you will need to read the job description to ascertain what they do. A lot of larger consulting firms use these titles and keep vague job descriptions because you might be moved from project to project doing different things. For example, I have seen analysts hired as a ‘cybersecurity

analyst' and moved into a role where they are writing reports for risk and then moved into a role where they are writing documentation for a 'future SOC'. Most of the time, people in the lowest rungs do not have control over what they do unless they have a high level of executive sponsorship or someone senior backing them.

Should I freelance?

If you are good at what you do, have talent and a passable level of interpersonal skills, go for it. But prepare yourself for an inconsistent income and high barriers of entry. This is especially the case if you do not have a consolidated reputation in the industry and no prior work to show for it. Most companies flock like sheep with products and service providers. If they hear one company in their sector and within the same size uses it they will generally flock and use it too.

Bug Bounties

Bug bounties are where you try and find vulnerabilities in a security product or a website. These are often publicised by the companies that have them with a guideline of what is in scope and what isn't. Two things to remember here. You can do bug bounties while working for your company given that the contractual clause does not state that all work done while being hired is owned by the organisations. There are penetration testers that have developed tools and have found bugs and had the organisation they work for claim it as the 'organisation's'. If you have confusion about your contract, speak to a contract lawyer.

The second thing is, there is fierce competition and a lot of work with not

much fruit unless you know what you are doing. If you write a fuzzer, be prepared that there are people with better fuzzers. If you want to write an exploit for a software, there are people who may be better reverse engineers than you.

Finally, the last point is, companies will try and argue against the bugs you find and try not to pay you. There are several instances where reputable companies have decided to say it is not a bug, argue against paying the researcher and then just go and patch the bug anyway. If getting payment is important to you, I would consider finding a job that lets you find bugs and get paid on the side at the same time. This will at least guarantee you a steady income stream. If you are doing this for clout, then go ahead.

Step 2: Building skills

Nobody knows everything. But if you want to work in cybersecurity you need to be aware you are signing yourself up for a career that demands life-long learning. The first thing I want to point out is that you need to be aware that universities, while great in giving some initial exposure, has likely not equipped you with real-world knowledge and experience. Secondly, your experience spending time on HackTheBox or other capture the flag challenges also does not mirror what the real deal is. In saying this, if you have worked in IT or a similar field, you are probably better positioned than somebody who does not know basic IT.

Nonetheless, the first step is recognising that there is some work to do and some things you need to learn. That is what this step is about. I am going to break down the pre-requisite knowledge and how you can acquire this knowledge for free.

Does a degree matter?

No. You do not need to have a degree to get into the field. Almost all jobs will say “Bachelor’s degree minimum” or something of the equivalent. This is not a pre-requisite at all. I do not have a degree, neither do almost half of my friends who hold very senior positions in some of the largest cybersecurity companies. All of these people earn well over six figures and have never had an issue getting a job because they did not have a degree.

People who think degrees matter have a narrow-mind and are a bit old school in their way of thinking. Most security professionals know that a degree does not teach you anything that is required in the day-to-day profession. How do I know that if I am a drop out you might ask. I used to work at the University of Sydney as an academic tutor for a master’s cybersecurity class and also an undergraduate cybersecurity class. I know the syllabus back to front. I also did computer science at the University of Sydney and took all the cybersecurity classes that they offered. These classes give you a glimpse into the cybersecurity world but really aren’t aligned with what the day-to-day job is like.

So the question then is why do job advertisements still put degrees on them? There are two reasons. The process behind writing a job advertisement is tedious. The honest truth is most companies do not write them properly. For example, when we were hiring for incident responders, we just took a template job advertisement that we use across the company, tweaked it a bit and put it up. Most of these templates are quite old and have that degree requirement on it. The second reason is because putting a degree or equivalent gives people an indication of level of knowledge that is required as a baseline. If you know everything already that would be taught in a

typical degree, then you should still apply as long as you can demonstrate this knowledge in a tangible manner.

Mindset Matters

Cybersecurity is not the hardest thing in the world, but it still takes work. You are going to encounter a lot of roadblocks and have moments where you might want to give up, but you need to learn to develop some resilience and push past that. The hardest part of getting a job in cybersecurity when you don't have that much security experience, or your only experience is a Master's degree or Uni degree is that your experience probably hasn't taught you enough to land you a job. That's bad form on the part of the education system, but also on the part of job makers because it takes up time and energy to train someone who is new. That time and training translates into dollar signs. The system is at fault, but so are the people unwilling to push for change. As such, prepare yourself for a long road that is going to be filled with peaks and troughs. You have a long road ahead.

When I wanted to get into cybersecurity, I knew nothing. One of the ways I shortcut my success was that I recognised how people are recognised and rewarded in the industry. The more you know, the more information asymmetry you force, the more value you bring to an organisation. This means developing yourself in a niche and being known for something and being known to deliver results. I realised if I cut out time every night studying or building on my skills, it was just a matter of time before I could smash out every technical interview. I knew there were not that many people who were skilled in reverse engineering or malware development. The reason is this is a tight niche and people do not want to go into it because it is tedious. I chose this niche because it seemed fun to me and I wanted to

use my programming skills.

Building a niche and being known for something is very important if you want to shortcut your success. It is all good and fair to be good at all areas of cybersecurity, but you want to be the person that is called upon to solve 'X' specific problem. If you are known for being one of the best at solving that problem, everybody will go to you – this increases your value in the field and helps to build your reputation.

So where do you start? If you are at ground zero and know nobody and don't have connections. You start with yourself. Be brutally honest about your strengths and weaknesses. How well do you know each area of cybersecurity? How would you rate yourself? Would you hire yourself if you were an employer?

The second point I want to stress is, stop coming at it with a mentality of "if there is someone who will take a chance on me I will succeed". For you to be in that position, you need to have something to offer. There are a lot of IT administrators, there are a lot of computer science graduates, there are a lot of masters students and PHD students with impressive research. That does not mean they will land a job. You need to focus on differentiation and making yourself someone that can add value to a company. If you evaluate yourself critically and work out what kind of value you can being to the company.

Your pay and worth as an individual to a company is directly proportional to the value that you can bring. Think about all the skills you've picked up. Can you program? Can you manage people? What can prove this? You cannot state skills in these without having some kind of historical evidence that can back it up. If you can program, are there programs you've written, do you have a GitHub page, have you contributed to a security project?

If you do not think you have any skills, this is okay too. It's time to build them and this is what this entire chapter is about. If you find a way to master all of these skills, you will no doubt smash the interview.

Fuck the 'try harder' mentality

If you are stuck with learning something, or do not understand something you are learning. Reach out to people. It's hard doing this alone. You will find most of the time people are willing to help you. I am more than happy to help anybody that has problems learning something or is struggling with something. I do not know everything in the world, but if it is something I can help with, I am happy to. Everyone started somewhere and I believe cybersecurity professionals should foster a community where we all raise each other up.

To demonstrate this point, back when I was a newbie and did not work or have any experience in the field…I have sent cold emails to people that I did not know, asking for advice or how to learn things I was struggling with. They have always responded.

With this, I want to reiterate my point. You are not alone. I love the cybersecurity industry because there are so many kind people in it willing to help you and teach you. If you need help or are struggling with things to learn or study, reach out. Reach out to me. If you don't want to reach out to me, reach out to somebody else. I am sure people are willing to help you. With that said, if you have questions about risk frameworks you don't understand… perhaps consider asking someone else, I do not know anything about risk and would just be as lost as you and would not be able to give you good advice.

How to learn things

It feels very strange writing a section about how to learn, but it really is hard when you need to teach yourself a completely new skill because it can be overwhelming when you don't know where to start. I think the first thing to remind yourself is, if you are new to security or you don't know much about 'hacking' or 'incident response', every skill can be acquired. If me and countless others can teach themselves a skill from scratch, so can you. You need to just set goals and break down what you need to learn in sizeable chunks. Make sure you are consistent in what you do and remember it is just a matter of time before you learn it.

There are several free resources that are available online that you can use. I learned a lot of my skills from three things – YouTube (it is almost embarrassing to say this, but I enjoy watching things and this helps me learn – and also, people tend to make videos about everything, I have even watched videos of people showing how to collect rocks), blogs and by re-creating situations myself.

After figuring out my weaknesses or what I am not good at. I think about what I want to become good at. After you know where you want to focus, you should write up a plan of how you can build those skills. This includes looking at syllabuses, talking to people in the industry and also following your general interest. I tend to use this to build a step-by-step list of the skills I need to acquire. I then work out how much time I can dedicate each day/week depending on the schedule and I set markers to calculate how much I have learned. This technique works for me, but you might find a better way that works for you. How you do this does not matter, what matters is you figure out the best way that can allow you to achieve your

goals.

The free resources that you can use include the following compilations:

- Learning how to hack - https://github.com/alex-bellon/cybersecurity-resources
- General cybersecurity resources - https://github.com/fabionoth/awesome-cyber-security
- Learning cybersecurity - https://github.com/CSIRT-MU/edu-resources
- Academic resources - https://github.com/onlurking/awesome-infosec

There are so many resources out there. If there are cybersecurity researchers or professionals that you like, most of them will have some kind of blog. You can read their blog to keep up to date with what they are doing. A lot of the security community use Twitter, so you can also use Twitter to follow people and keep up to date with what they like.

Work twice as hard

If you want to fast track your career and be a ‘better’ hire or ‘more technical’ than others around you, there is NO shortcut. You need to put in the hours. Nobody is naturally born able to reverse engineer or hack into industrial control systems and understand all the networking protocols. Everybody started somewhere, and you can achieve it too if you stay determined and willing to put in time.

If you work twice as hard and more effectively than someone else, there is no way you will not be earning more and more technical than them in half the time. The way I fast tracked my career personally is I worked my ass off in my spare time. I realised if I learned things and built my skills outside of work not just during work hours, I can speed up my technical skills and

experience.

I decided to make a list of all the things I did not know but would make me a ‘more rounded’ cybersecurity professional. This is why even though I work in incident response, I know how to break into things, and I have even done red teaming in my career where I have broken into companies, physically messed with the networks and gotten enterprise administrator (highest level of privilege). Cybersecurity across all the different job descriptions is actually a lot more interconnected. If you are a professional who understands threat intelligence, knows the threat groups, the tools and techniques highly sophisticated threat actors use, and you know how to do what they do in a red-teaming/penetration testing standpoint and also know how to detect and respond to it – that to me, is the absolute package. This is my personal philosophy and I know some people will not agree with me, but it was completely pivotal to how I have ended up where I have ended up in my career in a short time.

It was important for me to fast track my career because that was one of my personal goals. I knew when I was at ground zero, the only thing holding me from being nobody in cybersecurity, to holding a good position was my knowledge, my experience and my ability to articulate. I also recognised, with effort, time and determination there is no reason why I could not get there.

If you do not learn things and never upskill yourself. Recognise, that there are people who are passionate in this field who constantly do. You are most likely never going to outrun them or out-compete them. You’re probably looking at a very long career trajectory because genuine passion always wins.

Study Guide for Absolute Beginners

There is a cybersecurity subreddit and I see some of the worst advice being dished out there. The most common advice I see is people saying, “learn how to code” or “learn networking”. Although having coding and networking knowledge helps you in the field, I do not think this helps a beginner learn about cybersecurity. For example, networking helps with an IT role and coding helps if you are making tools. But learning how to code doesn’t teach you about the kind of problems you might be solving in security and learning networking does not necessarily teach you the vulnerabilities that come with networks and security flaws that exist.

I think for most beginners, a good place to start is to learn the basics and start with things you already have access to. For example, your desktop or laptop.

Things to Learn

These are taken from the GitHub links provided above for free resources. If you have already done these, please refer to the GitHub links for things to further your education.

- CompTIA Security+
  This course covers general security knowledge including security in an organisation, how security is set-up and some cryptography. I think this is a great starting place for someone who does not understand anything about security.

- Introduction to Computing Fundamentals
  A free, self-paced curriculum designed to give a beginner all of the foundational knowledge and skills required to be successful. It teaches security fundamentals along with building a strong technical foundation that students will build on for years to come. **Learning Objectives:** Linux, Hardware, Networking, Operating Systems, Power User, Scripting **Pre-Reqs:** None
- Introduction to Capture the Flags
  Free course designed to teach the fundamentals required to be successful in Capture the Flag competitions and compete in the picoCTF event. Our mentors will track your progress and provide assistance every step of the way. **Learning Objectives:** CTFs, Forensics, Cryptography, Web-Exploitation **Pre-Reqs:** Linux, Scripting
- Introduction to Security
  Free course designed to teach students security theory and have them execute defensive measures so that they are better prepared against threats online and in the physical world. **Learning Objectives:** Security Theory, Practical Application, Real-World Examples **Pre-Reqs:** None
- Practical Skills Bootcamp
  Free course to introduce students to Linux fundamentals and Python scripting so that they "Learn Just Enough to be Dangerous". Fastest way to get a beginner up to speed on practical knowledge. **Learning Objectives:** Linux, Scripting **Pre-Reqs:** None

Study Guide for Aspiring Penetration Testers

If you are looking for a role in penetration testing and have no idea where to start. The first step is to familiarise yourself with Windows and also Linux operating systems. There are a lot of resources to do this with. Most users will be comfortable with Windows – but if not, you can download disk images to play with from the Microsoft website. This is a list of items to learn that have been recommended by several penetration tester colleagues of mine:

- How to set up a virtual machine (VMWare or VirtualBox)
- Setting up Kali Linux on a virtual machine
- Linux Operating System
- SSH
- Basic python
- Active Directory Attacks
- Authentication mechanisms
- Networking (consider doing CompTIA Networking)
- Hacking web applications
- Basic command line
- Basic cryptography
- Tools on Kali Linux
- Bash scripting
- Evasion techniques
- Privilege escalation tactics
- Using exploits
- Password attacks
- Brute-forcing mechanisms
- PowerShell
- Penetration testing methodology
- How to use the tools in Kali Linux
- HackTheBox challenges
- OverTheWire challenges

Study Guide for Aspiring Blue Teamers

If you want to work in a blue team doing threat detection, threat hunting or SOC analysis, here are some basic things you should make sure you are familiar with before you proceed.

- Mitre Att&ck framework
- Different types of incidents (phishing, insider threats, web exploits etc)
- Active Directory
- Windows internals
- Linux operating systems
- Basic enterprise architecture
- Networking
- Indicators of compromise
- OSINT
- Basic malware analysis
- PowerShell
- Command line
- Basic bash scripting
- Python
- Basic IT administration
- Detecting lateral movement techniques
- Exfiltration techniques
- ELK stack
- Log analysis
- Process analysis
- Incident Response process
- Attack groups and their TTPs (tactics techniques and procedures)

- Wireshark
- Packet analysis
- Yara rules
- Attack tools
- Malware families
- Hashing

Study Guide for Aspiring Incident Responders

I truly believe if you want to be a great incident response consultant, you need to already be a proficient blue teamer. This means if you were placed in a blue team role, you would excel in that position. Incident responders also need to have a strong understanding of threat intelligence roles and how threat actors operate. This informs some of your response choices and priorities. I could go on all day about what to learn to get into incident response, but understanding the below as best as you can get you kickstarted:

- Threat actor knowledge
- All of the above for blue teamers
- Windows forensics
- Linux forensics
- Network forensics
- Malware analysis
- Memory forensics

What to spend time on

If you already know everything in the guides above, then think again. With

every single one of these dot points, you can go deeper and deeper. The more you learn you will realise the less you know. I would try not to get too overwhelmed by just how deep the subject area goes and how much ground you need to cover. The most important thing here is just to keep learning. Slowly over time you will be able to look back on the work you did and realise just how far you have been able to come.

Certifications?

You do not need to have any certifications to be successful in this field. There are so many people in this industry that do not have a degree nor any certifications and have managed to be wildly successful. Certifications are great if there is a company that is willing to pay for your education as it essentially forces you learn, but they are absolutely not necessary.

Please do not look at somebody with a lot of certifications and assume they know all that information either. People tend to forget things they do not use, and there have been many instances during interviews where people have impressive credentials but did not retain anything from it.

I would approach certifications this way. For me, I did not have a university degree and I also did not have any certifications when I had a six-figure job in cybersecurity. I only decided to pursue certifications because it was a way for me to prove that I already knew everything that I knew. I also only got certifications because the organisations that I was working for paid for them. The first certification I did was the SANS GCFA. I paid for that by doing the SANS work-study program as the company I worked for didn't fund it and I also could not afford the massive entry fee. The work study program is where you volunteer to help out and they give you the course at a discounted rate.

The question I guess becomes, do my certifications help me get paid more or noticed more by employers? Yes and no. I do not think I get paid more because I have certifications. I think I get paid in proportion to how much value I offer and how I demonstrate my technical and social ability. In terms of does it get me noticed – yes, by recruiters who search keywords on LinkedIn. Is this a good thing? Yes if you can prove you know what you know. If you get in the interview room and you freeze up or fail to demonstrate your knowledge, then I do not think this is very useful to you.

My position is this. If you are time poor and your company is willing to fund a certification for you, then do it because you have nothing to lose. If you can teach yourself everything and stay motivated, then I don't see a need. The question then becomes how can your resume reflect that you know this knowledge and get noticed? That will be covered in step 5.

Focus on learning and building your skills. Try not to focus on anything that might be a vanity metric, because when it comes time to be tested, it becomes very obvious if you know what you're talking about.

Step 3: Networking and building reputation

My goal for this section is to relay some advice about how to start from ground zero. This is if you don't know anybody in the industry and don't have a reputation for anything. There are things you can do to start laying the groundwork and cement yourself in the security community. The plus side of this is, the security community is small, so if it does not take long

for you to get to know people and become embedded within the community.

Build digital proof

Let's say you do not have any 'experience' in security. You might have a degree, no certifications or you might have no degree and no certifications. You can show 'experience' in other ways than just job experience. What I mean by this is having something online that demonstrates your knowledge. This can be a blog, a twitter account, a GitHub, presenting at University, presenting at a workshop, speaking at a conference, winning a CTF, participating in something at a conference, the number of boxes you've hacked in HackTheBox – honestly, anything that you do online security wise that can be recorded or tracked in a tangible way, works. The reason why digital proof is so useful is because it shows skill, and it shows hiring managers genuine interest in a subject and an ability to learn.

Having digital proof is also not mandatory if you do not want to do this. However, it is something to consider if you have no experience, degree or certifications. The reason I mentioned this is because I have seen a lot of colleagues around me get hired for this premise – their digital proof demonstrated skill and landed them an interview.

For me personally, when I applied for jobs the only 'proof' of skill I had to my name was a blog with some random writing I had done when I was trying to learn. And let's be honest, I do not have a forte for writing, so my blog posts are not written very well! My blog honestly landed me my interviews as I had hiring managers ask to read the blog – or email me asking me for links to specific titles. During my Accenture interview, my manager even told me that he had read my blog and found it very interesting.

I did not have a lot to put on my resume as obviously I had no experience doing anything, so I had a section on my resume I titled as “publications / writing” and had links and titles of blogs I had written. I will go more into things you can do with your resume in the later steps.

During university, in my spare time I had programmed a lot of fun side projects that were security related. These were not ground-breaking things I built but were small scripts I would use to crack something or break into something. I also had these listed on my resume.

If anything, I implore you to have a little think about what digital proof you have. It can even be a university project you have done that is linked to something security related.

How to use LinkedIn

I hope you have a LinkedIn for a start. If you do not have a LinkedIn perhaps consider getting one? The reason is because a lot of recruiters, events and discussions take place there in the cybersecurity world. I love using LinkedIn to see jobs that are available and all the jobs I’ve applied for I have found through LinkedIn. Also, I receive several job offers through LinkedIn because hiring managers are always searching through LinkedIn for keywords that might bring them to your account.

I am not a social media specialist, but if you want, you can take a look at my LinkedIn as it’s managed to land me a lot of job offers. But in general, there is an oversupply of jobs in security and not enough talent. I have some LinkedIn tips that I don’t think everyone will agree with – but these are more to do with my personal values more than anything. If this doesn’t align

with what you want to do, please feel free to ignore what I am about to say.

This is what worked for me. There are many strategies you can use, but I'm here to just relay my experience. Personally, I aim to have a LinkedIn profile, resume and other social accounts where someone can tell what I am about within 10 seconds or less. I make it very obvious and strive to use the least amount of words possible. I do not like wasting words or rambling more than I need to. The reason for this is people do not read those biography paragraphs people write on their LinkedIn and resume. They do not have endless time and most of the time hiring managers are viewing hundreds of accounts a day and they are not going to read everything you write. As such, I think you need to make it very obvious and explicit what you are about, otherwise sometimes if you write too many things sometimes, they become confused about what you want to do.

I don't see value in writing a biography paragraph telling people you are "an outstanding" or "excellent cybersecurity professional". Obviously, nobody in their right mind would write "I am a terrible security professional". To me, those adjectives are redundant and should be removed. The second point is, I think you should use your biography and headline to explain what you are about. For me, I only care about forensics and incident response so I spell this out very obviously in my headline. This way all the jobs I get are always for blue team related roles. Hopefully, you've completed Step 1 and are clear on what you want to do and why you're here.

There is a lot of advice on LinkedIn that you need to put keywords everywhere on your LinkedIn. Please don't overdo this, it comes off like a foreign language and makes you not seem like 'serious' candidate. To me, it gives me the impression of someone who doesn't care what job they get, and they use it to 'catch' all opportunities. I think you should show your personality and what you are about in your LinkedIn – this does not require a paragraph about why you like fishing or how passionate you are about

security. Simply, think about factual things you've done – your digital proof. Remember, everything you say about yourself needs to be 'backed' by evidence. It's more compelling to show you are good at something, versus telling people you are good. An example here is, I don't need to tell people "I can do forensics", I show them through blog posts or my experience.

When I did not have experience, I knew how to program in several languages, and I had proof of these in the form of GitHub and projects and programs I had written. These were the kind of things I had on my profile. I also knew about AI and had written a research piece that classified images. I had a link to that piece of work on my profile as well.

With this, if you have done several CompTia courses or other courses equivalent, please do not shove all of this in your headline especially if it goes on for too long. I think things like this fit better in the 'Education' section of LinkedIn. Reserve your headline for only a few points, i.e. what you are about "Aspiring Penetration Tester" and then have a few credentials after that. Think about what kind of penetration tester you want to be – or, if you're a red teamer and you're good with physical security, I would specify this in your headline or bio.

Another piece of advice I have is look at peoples' profiles. Find people on LinkedIn using keywords – for example, if you like red teaming, search "red teaming" and have a look at the profiles of professionals that work in the field. Once you see around 10 or more, you will start to see a pattern and hopefully be able to discern from a good profile to a bad one.

If you are unsure if your profile is good or not, you can reach out to people. Speak with hiring managers, ask for feedback. People are willing to help and if you have a profile on LinkedIn and you don't know if it's good for incident response, ask me or my colleagues, we will try our best to help

you!

Relationship with recruiters

Should you have a relationship with a recruiter? For me personally, I have never gotten a job through a recruiter, but I have great relationships with recruiters. I have applied to a few jobs through recruiters when I first started out, but those jobs were not the right fit for me. My relationship with recruiters tends to err on the more friendship side, where I might have questions about the job market, candidates – and they might ask me if I know anybody for a role that they have advertising.

On the flip side, some of my colleagues have gotten jobs through recruiters and this is a totally valid method of getting a job. In this situation I think you just do what is right. If you want a job that a recruiter is advertising, you have nothing to lose by reaching out and speaking to the recruiter. A thing to remember is they want to help you and they also want to find the right fit for the role they are advertising, so they are willing to help address concerns about your resume or the role if you have any.

For life in general, there are some terrific people and there are some not so terrific people. I would use your common sense and best judgment for whether or not a recruiter has your best interest at hand. There are some fantastic recruiters who deeply care about the people they're fitting for a role, and vice versa.

If you don't know any recruiters, you can look for them on LinkedIn. Most of the time a few keyword searches will land you with recruiters in the industry. If you don't know how to do this, you can also ask professionals in

the industry for recruiters that they recommend. Then, once you have that recruiter's profile, you can add them as a connection and send them a LinkedIn message introducing yourself and why you added them.

Industry Events

There are so many different kinds of industry events globally that you can attend based on what you are interested in and where you live. There are even security-based support groups for various different causes i.e. women in security or people of colour – just to name a few. You can find these typically advertised on LinkedIn, or even by visiting meetup.com and searching for cybersecurity.

Three events I highly recommend for people who are new in the industry are to attend SecTalks. There are global SecTalks that run monthly across the world from Australia to Netherlands, Brazil, Korea, NZ, China, Germany, Slovenia and the UK.

The second event is Bsides, this conference happens annually all over the world and is a great opportunity to listen to talks, participate in CTFs and meet new people. I have attended Bsides knowing nobody and have come out of it making new friends.

The third are the SANS community nights that are held all over the world. Industry professionals will often present talks or research into a subject and you are invited to join and attend. This is free for people to join and is a great place to meet like-minded people interested in the same subject and also to meet key industry professionals.

There are so many other fantastic security conferences that occur all the time that I would also highly recommend but I think the important thing to note is that, if you have an interest, no matter how niche, there will be a conference for you. There are several conferences held globally for malware reverse engineering and also physical security and threat intelligence summits.

If you cannot afford to attend a conference that is not free due to travel or monetary constraints, there are several programs you can join. Most of these conferences have programs you can apply to for the conference to be fully paid for, just look out for these on the website. If you do not manage to get accepted into the program, don't worry! Often these conferences set up a slack group, or a social media group you can still participate in and connect with people on. Most of the time they also upload video recordings or slides on their YouTube channel or social media pages that you can download.

When you go to an industry event, keep an open mind, be friendly and try to approach people. If you are painfully shy, the best way to meet people is to contact someone who is also going to a conference and ask them to introduce you to people. If you absolutely know nobody, try to attend an activity like a lock picking room for example, and you will instantly meet people who are seated at your table.

Should I write a blog?

For me personally, I write a blog because it's a way of tracking things I've learned, sharing things that I have done and building some digital proof of my skills. I don't blog very often because I don't enjoy writing (do you see

the irony!). But my blog has managed to help me get my foot in the door for a lot of interviews, so I don't see a negative side of the blog.

One hurdle that I think people struggle with is they think 'why would anybody want to read what I write?' or they think they don't know enough to write anything useful. You need to stop this way of thinking and just realise that blogs that are written by people who are still learning tend to be much more useful than a blog written by someone who knows everything. The reason is, if you are learning and documenting your knowledge, someone in the same boat might stumble on it and you might help them. Also, having a digital record of what you are interested in, what you learn and what you spend time on are things that hiring managers look on favourably because it really shows you are interested in the subject.

With all this said, if you don't want to write a blog you don't necessarily miss out on anything. You just need to find what works for you.

Twitter

A lot of cybersecurity professionals operate on Twitter. I've made a lot of friends through Twitter just by commenting and following people. It's a great place to get security news and understand what is happening. Often security professionals post their research on Twitter over other social media platforms and they use Twitter to alert people of any new blog posts that they may have written. I have also seen job advertisements being placed on Twitter. It's a great place to see what other security professionals are doing in their spare time and what they are learning. I've had plenty of conversations with people just through Twitter!

More importantly, there are people who post a lot of knowledge on Twitter. I

have seen people land jobs because of the content they post with no prior job experience. If you demonstrate skill and demonstrate passion and you're consistent, there's no doubt you will get noticed.

Mentors

You do not need to have a mentor to become successful in cybersecurity. What you need is some kind of skill that can be useful to the places you want to work. I think naturally, people want to help others who show genuine interest and passion. This has been the case for people who have helped me along my career who have taught me things and also equal for other people who I have also tried to help.

If you want to learn from someone and have mentors who can guide you. I would say, just reach out to people you admire and respect. The worst they can say is no or that they don't have time. Most of the time they will respond and give you some advice that you can use to succeed.

Building reputation

Building reputation takes time and it takes consistency. Don't despair if you are unknown and if you have no reputation. Start small and slowly you will realise how far you have come. One of the most important things about reputation and being known for something in security is actually tied with how you are as a person. I truly believe that it's important to be kind and a good person or believe you are better than everyone. People tend to respect and remember people who are inherently kind.

In terms of your career and what you excel at. If there is something that you

feel passionately about and believe you can excel at, I would always point these out and make a point to let your hiring manager know this. When I was starting out, I made it a point to let my hiring managers know I loved malware. This passion for malware and threat actors turned into passion for incident response. The reason I didn't say I loved incident response is because I had not yet had a taste of it before I worked in cybersecurity. When people are made aware that you have a passion for something or care deeply about a subject area, they are more likely to think of you for a role where that is one of the requirements. Having passion for something really sets people apart from other candidates as it does not happen that often and when it does, it's memorable.

Another way you can build reputation is by contributing to an open-source project. There are tools that are constantly being developed in the security community who are desperate for more contributors. If you know how to program and enjoy building things, you should find project that aligns with your interest and ask if you can contribute to it. This looks fantastic on someone's resume as it is also seen as contributing back to the community.

Don't suck up

Please do not try and suck up to people to try and get a job. I have seen this occur and it rarely ever works out well for them. When you suck up to someone, you put them in a position of power it makes the relationship dynamic very awkward and strange. Please instead focus on demonstrating your skills and realising that you do have value to add. There are so many jobs in cybersecurity but not enough talented and skilled people. If you're able to show you have these skills and can fit a role, you do not need to suck up.

Cancel culture on social media

If you have a social media account that is publicly accessible, I encourage you to be careful and put some thought about what you want to share. All too often people get fired or 'cancelled' online over something that they shared which might not reflect who they are as a person. Your social media account is tied to you, your brand, and that is also an extension of the company you might work for. If you want to have a social media page that is personal and private that you don't want to be viewed by clients or people you don't know – I would suggest making those accounts private.

A lot of people in the cybersecurity industry use Twitter or LinkedIn as a dumping ground for relationship problems, complaints about their workplace or complaints about people in the industry that they dislike or have some problem with. Everyone is entitled to use their social media how they see fit. But just keep in mind that there might be potential societal consequences to what you choose to share. For example, if you publicise something that you dislike about your workplace or say something publicly about a mistake someone made or a manager you dislike, this might slip you into legal territory surrounding defamation for that person or defamation for the company you work for. I would check your contract and a lawyer if you have concerns over anything you might have shared.

Just remember, that if it's on the internet, that means it's public. Once it's out there, it's harder to take back. Just put some thought into what you say and keep this in mind when you use social media.

Step 4: Resume and applying for jobs

Before you apply for a job, there are things you should consider about yourself. I think it's important to always have some level of self-awareness. Know yourself, know your strengths and know areas that you can improve on. You should also spend some time considering what makes you different from other candidates. Everybody is naturally already different as our cultural backgrounds, environment, and experiences makes it so. If everybody had the same ivy league background, it makes for a very monotonous workplace with little to no diversity. Just remember, employers like diversity. Having a different background or a difference of opinion is actually a good thing. Most of the time, I see people who feel embarrassed because their background is different, and they think it is a negative thing or something to be ashamed of. This is not the case at all!

Consider skills you naturally might have. I am Asian and I can speak 2 other languages outside of English as English was my third language. This is a skill that employers will look upon as a differentiation point if it is important for the job you are applying for.

Shotgun approach

The shotgun approach is something I see boasted about on LinkedIn and I think is stupid. I see people boasting about how they "tried 150 times and finally got 1 job". I then see people in the comments being like "wow that is inspirational". Quite frankly, I see this as an extremely ineffective method and a complete waste of time. You honestly are not a 'stronger' person for being rejected 150 times, you are just someone who does not learn from their mistakes.

If you apply for 150 jobs – does that mean you have asked for feedback on

150 rejections and used that feedback to refine your process 150 times? Most likely not. Most of the time, these people have sent the same resume to 150 places with no level of thought or customisation. It is extremely obvious when people apply for a job just to ‘get a job’ and they don’t care about the job they are applying to. Their resumes tend to have nothing to do with the job and it’s also obvious they have not read the job descriptions. Applicants like this normally do not even make it to the interview process.

If you are in a place of desperation and you need a cybersecurity job and just want any job. Make sure that when you apply you read their job descriptions and you tailor your resume to each job you apply to. I have never applied to the same job with the same resume, ever. By doing so I have always managed to land interviews for the positions.

In my honest opinion, I believe in applying for the jobs that you really want and making sure that your application is extremely tailored and customised for that job. I have never applied for more than three jobs at a single point in time. I take a lot of time to find the right jobs that I actually am qualified for experience wise (even if that experience is anecdotal and just proven in blog posts) and then tailor my resume to make sure that it hits on every single dot point they are looking for. I want to stress here, DO NOT LIE on your resume. It is so obvious when it comes time for the interview and people have stretched the truth of their ability. This also does not help with your reputation… as people talk.

Differentiation

When I reflect on the hiring process, we went through at Accenture for people to join the Cyber Defence team, I remember just an endless number of resumes and only a few that stood out and landed interviews. When I

think about what made these resumes stand out, there are a few points.

The first point is their resume was targeted to the job advertisement. This means, if the job advertisement was for a threat intelligence role – their resume demonstrated interest or relevant experience to match threat intelligence. For entry roles that did not ask for any niche experience, their resumes had something that showed interest in cybersecurity. This can be the form of a blog or something they did that was security related at university.

The second point is their resume is uncluttered, easy to read and filled with relevant information. Sometimes people put a list of skills in their resume that goes on for pages and pages – half of it is redundant. An example of this is where someone might apply for an incident response role, and under skills, they decide to put that they can use Microsoft Word. I think the reason people do this might be because job advertisements might say that the role will include some report writing. I would expect most people know how to use Microsoft Word and putting this in your resume does not make you more hireable unless the role is focussed on someone who can use Microsoft Word (which in most cases it is not).

People tend to also write paragraphs that describe who they are and what their experience is. You do not need to go overboard here. You also do not need to use emotional language that is charged with adjectives like “outstanding” or “best”. If you write too much, I can almost guarantee nobody has sat there and read your resume word for word. Remember, first impressions are made within seconds. Your resume needs to communicate “I suit this role” within seconds. And if it is filled with paragraphs that are hard to skim through, that first impression might not be one you wanted to give. Instead, focus on hitting the main points in the job description.

Make sure you highlight things you have achieved in your life that is

relevant to the job. You do not need to write about how you were the best car washer in a car washing company. That is completely irrelevant. Personally, I would leave jobs like this out. Before I worked in cybersecurity, I worked a lot of jobs to pay rent. These include working at a clothing store selling clothes, working as a bank teller and other roles like this. I chose not to put the fact I worked selling clothes because I think this made my resume seem completely not tailored to the job I was applying for. I also did not put down that I was a bank teller as this also did not feel relevant. Instead, I made my resume focus on security related things I had done, programs I'd written, projects I had worked on during university and blog posts and research projects I had done.

This principle also works for jobs outside of cybersecurity. One of my closest friends has two university degrees and wanted to get a job in Venture Capital but normally that is not a job you land right out of university. He had zero job experience. Most people in that career path work in investment banking or something equivalent. He decided to apply anyway. Out of university he worked in a supermarket and was also collecting unemployment pay checks from the government. These are not things he put on his resume. Instead, he filled his resume with relevant things he had done. In his spare time, he invested in bitcoin, traded stocks and had a lot of companies and areas he thought should be invested in. This is what he put in his cover letter, and also on his resume. This landed him two interviews – one with one of the best Hedge Fund managers in Australia, and the second an interview with the most profitable best venture capital firms in the country – which is where he works now. That job had several applicants ranging from PHD students to people who were extremely qualified. What made him get the job? Demonstrated passion, demonstrated skill and talent. This is what he filled his resume with, and what helped him land the job. There are people out there who are willing to take a chance on people with no experience as long as you have skills and *think* in a way that suits the role.

This section might seem so obvious to some people, but you will be surprised by how many people make mistakes and send resumes that seemed like they copy-pasted.

Transitioning from IT to Cybersecurity

There are a lot of IT professionals who are looking to transition into cybersecurity. If this is you, you're lucky, you already have industry experience and knowledge that is applicable and useful for a cybersecurity role. I think the biggest problem that IT professionals face is that their resumes are too 'IT' focused and not 'cyber' focused. What I mean by this is, their resumes are tailored towards landing a senior role in IT and it is irrelevant to cybersecurity. This can be seen in the listing of numerous IT systems and all the IT work they have done and the tools they know how to use.

I would advise these you to focus on any cyber related experience you have had and put this in your CV. For example, one of my friends came from an IT admin then to a server management role. In his resume, he put down that he dealt with security incidents that occurred on the servers and provided examples of this. In his spare time, he really likes to configure Linux systems and play with tools in Kali. Just put some thought into your background and think about how it links to cyber. For example, if you are a network engineer – have you had to analyse packets during an incident or look through firewall logs? These are all things that are 100% applicable to cybersecurity. These are the kinds of things you should be thinking of putting on your resume as obvious as it may seem.

LinkedIn Etiquette

The people that you see on LinkedIn are the same people that you might come across in the security industry. Cybersecurity is a small industry and people talk to one-another. When you decide to approach people on LinkedIn, treat them how you would treat a normal person who was standing in front of you, or a group of people in a room. You would not send the same message to 40 of them waiting for a response. You are more than welcome to message 40 people, but if it is a copy paste and you have spelt peoples' names wrong, then it doesn't come across like you care or are truly that interested.

I think a general rule is to be polite and professional. Try not to message people demanding things or sending their CV and asking them for a job (unless they asked for this). Think about the conversation like a normal conversation with a human and start off by introducing yourself and explaining why you are reaching out to them.

Lastly, don't be afraid to post things on LinkedIn. If you have done great work and you want people to be aware of this, you should post something on LinkedIn. This is a great chance for you to get 'noticed' as the more people 'like' or 'comment', the more that is shared with their respective networks. Even if it is an assignment you just wrote that you are proud of, or something you did in networking, post it. If you do not speak up about things like this, nobody will know.

Try not to over post low-quality content. There are a lot of people on LinkedIn that constantly post news articles or inspiration quotes. If this is the kind of person you are, go ahead, but personally for me, I believe in

quality over quantity. Try to put some thought and effort into your posts and work on trying to ‘show’ some personality and who you are through them.

Finally, LinkedIn is not a professional dumping ground where you should post rants or anything too personal (fights with significant others etc). Think about the context of the social media platform and whether or not what you are posting suits the channel. One kind of post that seems to gather attention from people are posts asking for advice. I notice when people ask for advice or experience from people, people are likely to share, comment and chip in. This is just human nature. If you have questions about getting hired or want someone to review your resume or just general resume tips – don’t be shy about using the power of social media to ask. I promise you nobody will look down on you or think less of you, and you will probably find that other people in your network will probably be thankful you posted it as it might help them too on their journey.

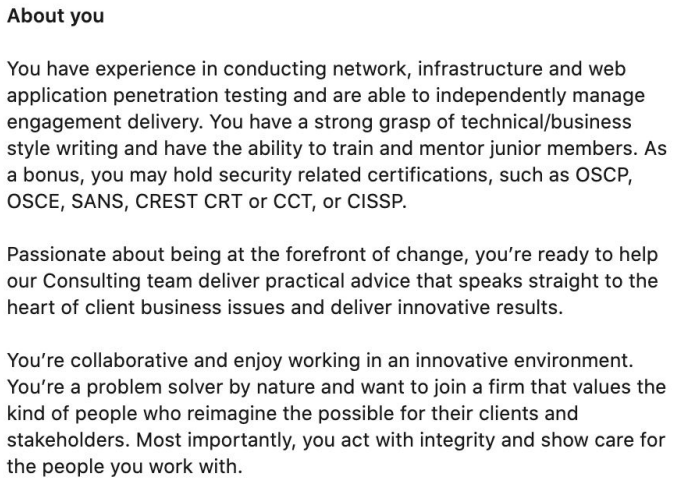
Reading job description requirements

In this section I’m going to show a few job descriptions requirements for various roles I have pulled from and describe what they mean and how to approach them. Remember that there are many skills that companies need, and you don’t know what skills they prize the most. The job description might have things you are not good at but that should not stop you from applying anywhere. Let the company make the choice if you are the right person or not.

Remember to always be honest and realistic about your skills. Do not lie or pretend you have a skill in something because it asks for this is the job description. It is very obvious later on in the practical interview or the

interview in general when this is the case. This will also leave a bad impression on you if you went through a recruiter and the recruiter hears this feedback about you. Further, the industry is very small, and people do talk to each other across companies. I have seen people asking each other if they know certain people and what their opinion on that person is. Foster a reputation for being honest and direct, even if this means you tell the person "I can work this out if I Google it". This is better for both parties in the long run.

Penetration Testing Role (Consultancy)



About you

You have experience in conducting network, infrastructure and web application penetration testing and are able to independently manage engagement delivery. You have a strong grasp of technical/business style writing and have the ability to train and mentor junior members. As a bonus, you may hold security related certifications, such as OSCP, OSCE, SANS, CREST CRT or CCT, or CISSP.

Passionate about being at the forefront of change, you're ready to help our Consulting team deliver practical advice that speaks straight to the heart of client business issues and deliver innovative results.

You're collaborative and enjoy working in an innovative environment. You're a problem solver by nature and want to join a firm that values the kind of people who reimagine the possible for their clients and stakeholders. Most importantly, you act with integrity and show care for the people you work with.

Source 1 - PwC Penetration Tester

Reading the job description pasted above, they are looking for someone with 'experience'. This does not mean you have been a penetration tester before, this means you know how to conduct penetration testing. If you have done hackthebox or other CTFs at home or at conferences, make sure you make this known. The ability to manage engagement delivery just means you can conduct a penetration test, write the report and deliver recommendations and findings to a client. It doesn't require that you've

done that before, but if you have a blog where you write-up your methodology or how you hacked into a box, this is the equivalent experience.

Reading the job description, they do not care if you don't have a degree or any certifications. This role suits someone who is junior who loves hacking and has hacked into boxes and played in CTFs. If your resume is heavily geared to this and you have a track record of hacking things (not just 1 box the day before you apply!), I think you can land this role and ask for a good salary.

Threat Intelligence Role (Large Consultancy)

What You'll Need

- You are proficient in English, both written and spoken,
- You can demonstrate experience in conventional network and/or host-based intrusion analysis,
- You are capable and comfortable communicating actionable threat intelligence to both technical and executive-level stakeholders
- You are comfortable assessing and producing cyber threat intelligence, open source intelligence or industry reporting,
- You have an excellent understanding of the Windows, Linux or OS X operating systems, and
- You are looking for a dynamic, fast-paced and challenging role in an unconventional team environment.

Additionally

- We highly value prior working experience in an area of cyber security intelligence,
- You should have a good understanding of current and emerging threats, and the ability to demonstrate practical knowledge of security research,
- You should have a working understanding of how various Governments carry out cyber espionage and for what purposes they do this,
- You can demonstrate experience in conventional network or host-based intrusion analysis, cloud security, or mobile device security.

Source 2 - Crowdstrike Threat Analyst

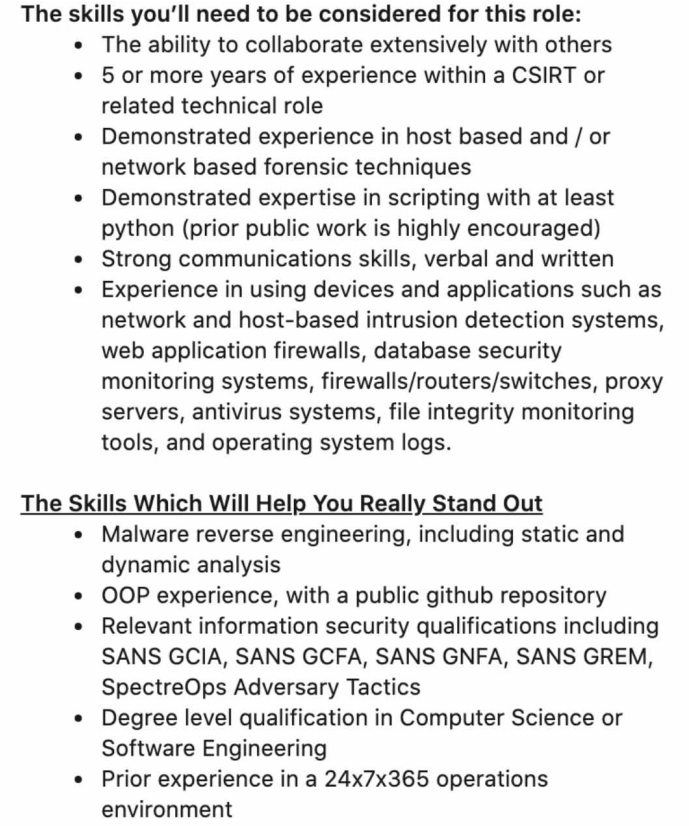
The first thing to note here is, if you are not good at English or you write poorly, do not apply for this job. The fact this is the number one point indicates that you are most likely going to be writing reports and potentially presenting to people in English. Reading the 'What You'll Need' section shows that this role will be highly focused on analysis of threats and also reporting. I think you will be tested on whether or not you can take one report or one piece of threat intelligence and communicate the most important points to someone technical, someone who is a manager and someone who is an Executive. This is not an easy thing to do for someone who is completely new to security. But if you are logical about how you approach this, this should not be too difficult.

They also are looking for someone who understands operating systems. I think this probably relates to the role as you will be analysing indicators that are collected from malware, network and other threat actor activity. This means if you are given an indicator which is a registry key, you need to know that is a registry key and what it means. I don't think they are looking for someone who is a forensic genius, but just core basics.

Reading the additionally, I think that you should also aim to show that you can at least cover 2 points. For example, for you to apply for this role you need to 100% have some level of understanding of cyber threats. This is not generic like "ransomware" or "phishing", but more detail. You should demonstrate some understanding of a threat actor group that you find interesting … for example a Russian threat group or a cybercrime group. Don't just detail what they did like a news article, but know about how to 'detect' them, what tools they use, how they do things and what their motivations and drive are. The third dot point shows that they are looking for someone with specific knowledge about nation-state funded groups. I would focus on studying about Russian, Chinese, North Korean and Iranian

threat groups. This is all knowledge that is publicised on Google. I think that if you do not know these things and if you can't demonstrate this knowledge you are most likely not going to get this job or an interview.

Incident Response (Large consultancy)



The skills you'll need to be considered for this role:

- The ability to collaborate extensively with others
- 5 or more years of experience within a CSIRT or related technical role
- Demonstrated experience in host based and / or network based forensic techniques
- Demonstrated expertise in scripting with at least python (prior public work is highly encouraged)
- Strong communications skills, verbal and written
- Experience in using devices and applications such as network and host-based intrusion detection systems, web application firewalls, database security monitoring systems, firewalls/routers/switches, proxy servers, antivirus systems, file integrity monitoring tools, and operating system logs.

The Skills Which Will Help You Really Stand Out

- Malware reverse engineering, including static and dynamic analysis
- OOP experience, with a public github repository
- Relevant information security qualifications including SANS GCIA, SANS GCFA, SANS GNFA, SANS GREM, SpectreOps Adversary Tactics
- Degree level qualification in Computer Science or Software Engineering
- Prior experience in a 24x7x365 operations environment

Source 3 - Salesforce Senior Incident Handler

Looking at this role, the first thing is, I would ignore that they want 5 years, it's okay if you have 3 years if you can demonstrate talent and technical knowledge akin to someone of 5 years. The word 'demonstrated' means they are most likely going to give you a practical interview to test your skills. The fact they want 'prior public work' means they want some coding proficiency and if you have a GitHub repository or some script or tool you've built, that is something you should include on your resume. The

requirement for experience using devices and applications does not mean they are looking for you to go and set-up these tools, but it means you need to know what they are, what logs they produce and what they do. It seems like the analysis of these will be important for the role.

I think to have the best bet at this role, you will need to be skilled in forensics in both windows and Linux. You should have some programming experience with proof to demonstrate this (preferably a GitHub repository). And lastly, if you can get one of those certifications that they have listed that will really boost your chances of landing this role.

Cover Letter

I do not think a cover letter is necessary at all. I have never in my life written a cover letter for any jobs I have ever applied to and I have gotten interviews. The concept of a cover letter is very old school, and some companies even write on their application that they don't want you to give them a cover letter as your 'resume says enough'. This is exactly the point here, if your resume has not said enough that you feel you need to write an entire letter about your application, then there is something wrong with your resume. Your resume needs to be concise, direct and communicate effectively why you are here. The 'why you are here' is not a paragraph of words explaining why you want the job, but your experience. Your experience can be a lot of CTFs you have done, or forensic work you experiment with in your spare time or malware that you have analysed or written about. That speaks louder than a written explanation of why you want the job.

Feedback

If your resume did not get you an interview, do not hesitate to ask for feedback. The truth might be that you just do not have enough experience or the skills that they are looking for. This is okay, this is something you can work on and can fix over time.

In general, if you are unsure if your resume is okay, ask people. You can ask industry professionals on LinkedIn, hiring managers and also recruiters. I am sure that all of these people would be happy to assess your LinkedIn and tell you the strong and weak points. When you do get feedback, don't forget to update your resume and try again. Try not to be one of those people who apply for 200 jobs and never ask for feedback and never learn what they could be doing to improve – both on their skills and also on their resume writing.

Take me for example, I struggle to come up with words to write because I hate writing. What this means is I often do not write all the good things I've done at work in my resume. I get my friends and colleagues to review my resume and they know what I do in my work and they often help me refine and update my resume. Feedback is a critical part of life in general and how you get better at things.

Bad Experiences

I know I have spent a lot of time writing about how if you don't have experience don't worry too much as people will still want to hire you. I want to use this section just to call out that bad experiences do happen and try not to take this too personally. Unfortunately, awkward situations happen, and unprofessionalism can also happen. Unless you instigate them, you should be glad you're dodging a bullet.

In one of my interviews, I was told directly by a Vice President in the final interview stage (there were 4 rounds) that my resume had red flags because why did I only have X years of experience but more knowledge than someone with X years' experience. (I am redacting the years for the privacy of the company). They proceeded to tell me how many years of experience they had and how long they had been working in security.

They told me I had done really well in all the rounds, but everyone was confused why I only had X year's experience and this was a 'major red flag' they could not understand. I realised I was not going to be hired because they could not 'figure out the reason'. This whole process was incredible frustrating and very awkward. Since they thought I had red flags from the beginning, why did they waste my time interviewing me and then confront me about it and imply that I'm lying?

They then ghosted me and did not tell me if I got the job or not. I had to chase them up for feedback and the feedback they gave me was that I was technically suited for the role but to "apply in 1 year so you have 1 more year of experience". They then reached out to me six months later trying to hire me for another role. They reached out via a personal email and also on LinkedIn. I did not accept.

That same resume passed background and reference checks and landed me several offers at other reputable organisations. I finally settled on a role in a place where they recognised my skill and were excited to have me on the team. I realised I had escaped a massive red flag. If I would've worked at that company, I don't think I would've been treated as an equal or paid for what I'm worth. I would be working with people with the complete opposite value and mindset to me.

This was no doubt a bad experience. But remember, that experience was a one off. There are a lot of open minded and wonderful people in security.

Just remember, there are people with 10 years' experience that have definitely earned their stripes and people with 10 years' experience that also have not. There are people with 0 year's experience who are gifted and talented, and there are also people with 0 year's experience who are not. Either way, if someone treats you badly or is rude to you, that's not a 'you' issue, that's a 'them' issue and their own insecurity. You're dodging a bullet and that company is probably one you don't want to work for anyway. There are 100 other companies that will most likely come at you with open arms and be excited to have you. Choose those ones.

Growth Opportunities

For me, my biggest goal in cybersecurity was to be one of the best in incident response. To be able to handle extremely difficult cases, to lead a team and deliver the findings and have happy clients. What this meant for me is, I needed to find roles that give me the maximum opportunity for growth and exposure to these situations. I also realised I needed to learn a lot and really push myself as there are a lot of talented and incredibly smart people.

To be able to work on large cases, you need to be trusted by your company. Your company trusts you when you have a proven record or technical skill that is consistent and can be counted on. When I look for jobs, I look for roles that give me this opportunity. I look for roles with a large growth upside, roles that expose me to different situations and challenge me. Money for me is always secondary. I think once you get good at something, the money comes naturally anyway.

Looking for high growth opportunities is a massive personal principle I

have. I apply this to decisions and choices I make. I always opt for the best long-term decision over anything that provides me short term relief. What this means work wise is, I always try to put myself in the most uncomfortable position, so I am always forced to learn. This means I try to take on some risk that is outside of my comfort zone. The reason I do this is because it stretches me, forces me to grow, forces me to learn and has tremendous upside for both your career but also your reputation. Granted, don't try to take on something you know you can't deliver.

This principle for me means I pay close attention to who I want to work for and who I want to work with. I always favour working for managers who believe in me, people who want to grow me and people who are open to giving me opportunities and things that are out of my comfort zone. When I apply for a job and sit through the interview, I always pay attention to who my 'manager' would be and ensure that I am able to have a conversation with them. I check and make sure we are on the same page and that there is some kind of synergy between us.

When you are applying for a role, you are also equally interviewing them to see if they are the right fit for you. Try to pick places that match your personal belief systems and work style. I have never accepted a job at a place where I did not like the manager or the culture. I have also never accepted a job where I can see that people are miserable or don't like what they do. These are decisions you should think about for yourself. Decide what values are important to you and what you want to look for. Think about your lifestyle and how work fits into it and find a job that suits that. Make sure you ask a lot of questions and work these out before you accept the job.

General Resume Tips

1. Read the job description about what they are looking for in a candidate and make sure your resume ‘answers’ each one of the dot points as best as you can

2. Don’t forget about your ‘experience’ outside work – things you teach yourself, CTFs you have participated in, research you have done, your GitHub repository. Include all of these things on your resume where it fits the job you’re applying for.

3. Show digital proof where you can – rather than listing skills, try to list skills and show proof of it. For example, if you like malware reversing, add a link to a blog post you have written.

4. Don’t write an essay about every job. Keep it concise and easy to skim-read. Put bullet points about your major achievements and what you did, but make sure these have been worded to match the job you are applying for.

5. Don’t stuff keywords everywhere especially when it does not make sense and is irrelevant. It looks cluttered and sometimes makes your resume appear ‘not serious’.

6. Do not spell your hiring manager’s name wrong or put the wrong company you are applying for in your resume. This does not communicate that you ‘care’ about the company and it comes off like you are applying for 100 companies at the same time.

7. Apply for the job properly via the website or where the job is posted. Do not message the hiring manager with your resume attached and expect them to type your resume up for you.

8. Ask for feedback. Ask for feedback on your resume from recruiters, hiring managers and professionals in the industry who are occupying the role you are applying for.

9. Apply anyway. Even if you do not fit everything they are looking for – demonstrated passion and skill is something that definitely attracts hiring managers.

10. Define what values you have and what you want in a manager and keep this in mind when you are applying for jobs and considering where you want to work.

11. You do not need to apply with a cover letter. Your resume should be sufficient enough given that you have communicated the “who I am”, “why I’m here” and “what I want” in your resume.

12. Don’t use adjectives like “outstanding” or “dedicated professional”. Show you are through examples in things you have done and your experience. These words are completely redundant.

13. Don’t write ‘etc’ on your resume. It communicates two things, and they are both negative. It tells the recruiter you have run out of examples but want them to think there are more examples, and it also communicates you cannot be bothered to spend time to list your other skills.

14. Don’t write random skills that don’t make sense. Do not group skills in a way that makes no sense either. For example “Skills: Nmap, Group Policy, Domain Administration, ISO 17024”.

Interpersonal Skills

Interpersonal skills are a very valuable asset in the corporate world. I have seen so many times where someone with good communication and interpersonal skills and bad technical skills gets promoted over someone who is technical. The reason for that is – the technical work is great, but if you cannot communicate what it means or the implication of it and make someone understand it – it's not very useful. Also, when you are working with a team and you struggle to communicate with your team members, this makes the job more difficult and stressful. It makes it more difficult to work in a team.

It is perfectly alright to be an introvert, have social anxiety or hate communicating. Cybersecurity is filled with people like this. I'm an introvert myself. I absolutely hate presenting or talking to people, but I do it anyway. This is just like hacking; it is a skill that you can learn and foster if that is something you want to do. If you want to be paid well, you will hit a point in your career where you will have to learn how to communicate. This communication can be in the form of verbal conversation to various people in different ranks, or it can be written in a report or colloquial conversations with colleagues. The better you get at communicating, the more suited you are to more senior roles that focus on management and have more touchpoints with executives and stakeholders. This also tends to grow with your salary.

On the flip side if you have zero interest in developing interpersonal skills and you would rather be left alone doing your own thing, this is fine too. I have also seen people like this in the consulting world who are more than happy just doing their own thing. Keep in mind though, most consulting roles will have a lot of customer touchpoints requiring interpersonal skills

so it may not be possible to avoid it entirely. Either way, ask the right questions in the job interview and work out if it's the right fit for you.

Dealing with Rejection

Rejection happens to all of us. I do not know a single person who has applied and gotten offers for every single job that they wanted. Everybody starts somewhere. Just remember it is a part of the process and do not let it get you down. Instead think of rejection as an iterative way for you to work out what is missing and try to improve on yourself. If you were rejected because there was a candidate who is more technical and has more experience than you, then think about ways you can learn those skills and get that experience. You can also apply for a job at a smaller company that does not have as much competition.

If you don't know why you were rejected, ask for feedback. The key thing here is to realise this is normal and to not feel bad about yourself or to give up. Just try to improve, try to learn more and keep going. At one point, almost everybody was at ground zero – with no experience and no connections. If people before you have gone through this, just know that you can go through this too.

Step 5: Acing the job interview

I can write a massive Russian novel about job interview questions and tips, but I am going to keep it short. There are so many different types of job roles in cybersecurity, so I am going to keep this section broader and give

some tips on how to study and prepare for each section. I am going to assume the place you are applying for will have a four to five stage interview. If it is only two rounds or three rounds, then lucky you! In that case just skip to the parts that are relevant to you.

Don’t lie and be a kind person

Do not lie in your job interviews. Don’t ever say that you can do something but obviously can’t because it gets caught out very easily and I have seen this happen. It will end up affecting your reputation in the industry. It’s a small community and people talk. When people apply for roles, it’s very commonplace that people ask around if someone knows ‘you’ and what their opinion of you is. I have heard feedback on people who have applied for multiple roles and about how they performed in the interview in terms of if they lied or if their technical skill just did not match their resume. If you end up lying and get caught by the interviewer, this feedback might be passed to the recruiter who recommended you and they might be reluctant to work with you again because that also impacts them. You’ve effectively wasted everyone’s time in that scenario. While lying or obfuscating certain things or elaboratively decorating ‘truths’ might land you interviews or even a job, it’s just a shitty thing to do and doesn’t speak highly of your integrity as a person. Somewhere down the track people will notice, and it will come out in consequences such as a slow career progression or people not ‘believing’ or pushing you for opportunities that come. More so, if you lie in your resume or during the interview, your ‘technical’ capability during the practical exam will raise questions about your resume. It’s far better to ‘outperform’ or ‘match’ what’s in your resume, than to fall short of what is written. If your resume is impressive but you fail to meet it, then it makes it seem like you do not retain information well and makes you far worse off than if you were honest and reflected what was written in your resume.

The second point here is to be a kind person. Do not step on people or play political games to trap or usurp them. You will be amazed how small this industry is and you might find that this person is a part of the interviewing team for a job you want further down your path. People talk and if you have a reputation for stepping on your team members that is not the kind of culture most people want to bring into their organisation. Stepping on people to get where you want has a limit to its effectiveness. It's far better to be authentically good at your job and a kind person who raises people up as you will reap the benefits that it brings. These benefits are reputation, word of mouth and other people who believe in you and want to give you opportunities.

Initial Call

This is normally the starting point of the job process. You apply and then you get a call from someone in the HR team or from the hiring manager for an initial interview. This interview is normally just a screening interview to make sure that you are the right kind of person before they proceed with the following interview process. There should not be any technical questions asked in this this conversation. Usually, this conversation will focus on questions about what you are looking for in a role, why you are changing roles, some questions about your background and experience and lastly, gives you more information about the role.

When you are in this stage, you should ask all the questions you have about the role at a higher level. Unless this person is a part of the team it is highly likely that they will not know anything too detailed about the day-to-day

activities. Instead, I would focus the questions more about team composition, values, work-life-balance, benefits of working there and the nature of the role. I normally use this as an opportunity to see how big the team is and I ask about the background of the team. I do this to assess my chance of getting the job if I am interested. My next questions always centre on the work life balance and also growth opportunities that are present in the role. The rest of the conversation then centres around why I am leaving and what it is I am looking for. I would try to be very honest here about why you are moving companies or looking to join this particular company. The conversation usually rounds off after 1 hour and ends on the next steps. This is a great time to ask this person about how many rounds there are in the interview process, how long the interview process will take and also roughly how many people are being interviewed. Some interview processes are very long and can be months… some are shorter and can be weeks. This is all useful information to know if you are applying for more than one job.

Sometimes, but not always, the question about salary expectations comes up here. This typically happens when someone has work experience already and this person is checking that they can afford you or you would be interested in the role within their salary bracket. Whether you choose to be honest or offer a range that you're in, is up to you. I don't think this changes the outcome that drastically because the later interviews in the process are normally what determines your pay.

Cultural Fit

When you're in the job interview, remember, you are also interviewing them to see if this is a company you want to work for. Ask questions about the people in the team, ask questions about the company culture and ask if there are team activities. The reason why culture is important is because you're

going to be spending almost all of your waking hours with this group of people and how they treat you, each other and how they approach their work will have an effect on you. What I mean by this is, if everybody in the team is overworked or frustrated at work, you are going to join a team that will likely be complaining or have colleagues who are already looking to quit. The culture and the team set the pace for the rate of work that gets done and how people are treated and accepted. If people at work do not care about their job and are just there for the paycheck, you might not find a lot of learning opportunities there or people who can support your growth.

During the interview, think about what values you have and where you want to work. Do you want to work more than 9-5, do you want to join a fast-paced competitive culture, do you want a mix of it, or do you want something a little more laid back? These are things you need to decide for yourself. Now, when you are in the interview, think about questions you can ask that might reveal this situation.

Some questions you can think about asking include asking about the churn rate – how long people stay on average in the current team and why they quit. I would also consider asking questions about work hours and how often people work overtime. In Australia, you should legally be paid overtime or be given days in lieu to make up for the time you have spent outside of your payable working hours. If you are curious about the team dynamic, you can also consider asking about what team building activities there are and how often the team get-together for non-work activities. At one of my previous roles, the whole team would spend Tuesday and Friday evenings together, get dinner or drinks. We were all very close friends and are still close to this day.

If you do not care about culture, then you can ignore this section. However, I think finding a good cultural place has a lot of benefits. If you find the right environment that values growth and honesty, it might accelerate your

learning rate and help you feel more rooted in the industry. If you are working somewhere that does not have the right support mechanisms in place, you might feel alone or lose out on an accelerated learning curve.

Again, these are all decisions you need to consider for yourself and to remember to ask the right questions that can help you determine if this is somewhere you want to work. Personally, culture is paramount to me. I will not work somewhere where I do not like the team and don't have a support structure. This might be different for you depending on your personality and personal preference. It is just something to consider.

Lastly, if you have trust issues and do not trust what the hiring manager is saying, you can always ask to meet the team. On two or more of the interviews I have done, I have been taken into the office and allowed to meet the team and also once was able to meet the team at an event. This is a great way to decide for yourself and see the people that you might be potentially working with.

Acing the Technical Interview

Normally, for a technical role in incident response, there are two components of the technical interview – a spoken interview and a practical interview that is time-boxed. This is usually also the case for large companies that are hiring for blue-team detection roles. For penetration testing roles, this can also be the case in some organisations. However, some of my colleagues have had an interview process where only the spoken interview exists. For threat intelligence roles there is always a spoken interview and a practical that centres on research and your report writing skills.

The technical interview for all of these roles are different. However, there are some tips I can give you to prepare for these. Before you start 'preparing' for the interview, think about your resume and some examples of stories that you have of your work that is relevant to the job. For me, I always think about 2-3 incidents that I have worked on in my career that are completely different to each other. I also think about some work experiences I have had that were tough – for example, difficult clients or work politics. The reason for this is, when you get asked a particular question, you should give your technical response, but it's even better if you back it up with an example from your experience. This gives you credit points and shows you actually have experience. Even if your experience is a CTF you have competed in where you have seen this.

An example of this in an incident response interview is: if I am asked a question relating to the detection of something running in memory – I can relate this to incidents I have worked that have required memory forensics and the output has revealed further insight to the incident. An example of this for red teaming that my friend had – they got asked a question about breaking 802.1X and they answered it with an example of a situation where he bypassed it through a meeting room phone and exactly how he did that. Answering with examples of work is always much more compelling than just a dry answer. It helps you turn the interview into more of a conversation (which is what you should strive to do) as it helps 'build' the relationship.

The next tip I have is to make sure you have re-read the job description and after getting a gauge of what the job entails in the initial call, you should have an idea of the broader questions you might be asked. In incident response, when the job advertisements have things like network forensics, host forensics, malware analysis, memory forensics, detection and networking. This generally means I am going to be asked detailed questions in all of these. If you are going for a Senior role versus a Junior role, the

questions go from being ‘higher’ level like “how do you detect if blood hound was used” to something like “how do you know a file is deleted if it’s been removed from the system and also in the recycle bin”. The second requires detailed knowledge about specific artifacts on the system.

Sometimes in a technical interview, you might be put through a ‘role play’ of something. For example, in incident response, you might be told “you’ve been told to lead an investigation of an Emotet outbreak, you are in the investigation lead, what do you do?”. The questioning then progresses to more things like “they have X logs but they don’t contain the information for the period in question… where else can you look?”. This requires you to go from the handling of the client and communications all the way through to how you investigate, how you analyse, how you deal with problems and how you solve the incident from start to finish. When dealing with interviews with this line of questioning, it’s good to take a step back and actually think step by step. The more detail you give the better. The worst thing a candidate can do in these situations is to jump to the endpoint without giving detail.

Remember, if you cannot answer all of the questions this does not mean you did ‘badly’. If you already knew everything for the role and answered everything perfectly that indicates that you probably should go for a harder role. If you don’t know the answers to questions, it’s okay to say you don’t know or talk about how you would approach figuring out the answers to that.

Finally, sometimes people in technical interviews like to throw massive curveballs at you and ask very difficult questions that are not even relevant to the job. You will most likely come across situations like this. When you’re in this situation it’s hard to be aware that it’s happening. An example is applying for an incident response role and getting asked ‘what is the best way of handling unstructured data in a database’. Personally, in those

situations I would just ask them if that is the kind of problem incident responders in their company face. Or, you can just reply or say you don't know and just evaluate if you want to work at that company.

Practical Interview Questions

As mentioned above, a lot of roles will give you a practical interview. This is like an 'exam' of some sort and is usually in a take-home format and timeboxed. For incident response, this might be some set of logs or a disk image and you're asked to 'find' something out or work out what happened. For penetration testing, this could be a time boxed CTF where you are asked to break into a web app or other systems and write a report on it. For threat detection this could be in the form of writing alerting rules to detect some kind of malicious behaviour. For threat intelligence, this is usually some kind of report on a threat actor or a piece of research they have asked you to conduct and to write a report on.

My tips on acing the practical interview stage that has some kind of 'report' would be to stay calm and write your answers or form your responses the way you would if you were speaking to the client. This means, make sure your responses are articulated well and written in full English. For practical exercises in incident response and penetration testing, I would make sure you are familiar with the methodology, tools and have done some variant of it beforehand. For incident response, you can run a malware sample on a virtual machine and work out how to detect it. For penetration testing, you can always practice HacktheBox exercises and practice writing a report for it.

My last point here is to try not to overthink it. Usually there is not some

hidden ‘trap’ in these practical questions designed to trick you. They want you to be able to do it and this is a great opportunity for you to see the kind of work you would be working on. I would take the practical interview as a fake ‘day-in-the-life’ of the job you are applying for. If you struggle to get all the answers or cannot answer certain questions, be honest. You do not need to be able to answer every single thing in the practical interview. This is the same principle as the technical interview – they most likely don’t expect the perfect answer for everything. Give it your best shot and I’m more than certain you will do great.

Drill down interview approach

This is a really common interview approach where you test how deep someone’s level of thinking is. I have seen this done in security interviews, software development interviews and also financial interviews. The way this works is, the interview will ask you about something broad, this broad topic is most likely something you have brought up yourself or have written on your resume. Take incident response as the topic, they might ask you about a case you have worked on or something you said you did on your resume. They will start of asking very broad questions about it – like “what was the nature of the incident?”, “how many people were involved?”, “what was your position in the incident?” etc. As you answer each one of these questions, their questions start to get more and more narrow. In this example, the line of questioning would go to “what did you uncover in your investigation?” and then to “what did you use to uncover that?” and “how did you know it was there?”. This can then go deeper and deeper to specific questions about a particular finding. Say for example, you told them you discovered that there were .LNK files with garbled names that had paths pointing to a piece of malware on the disk. They might ask you “what did

you analyse to determine how these were created?".

The reason why this method is so effective is because it catches people who lie on their resumes or pretend, they played a bigger role than they did on a project. It also helps work out how deep of a problem solver someone is or how deeply they think. For people who say their skill is that they love problem solving or that they learn fast, this is a good way to see how 'deep' this is. The way that they solved previous problems and the mental framework they applied to solve this problem is a good way to gauge how they might solve present problems they are given in the new role.

The only way I would suggest preparing yourself for this is to make sure that you are not lying on your resume and when you bring up experiences you are prepared to have these experiences dissected and talked about. This takes us back to an earlier point I made about prep-work for an interview. Always try to remember a few key experiences you've had before an interview.

Ethical interview questions

Depending on the seniority of the level you're applying for, you might be asked ethical interview questions. These questions tend to centre on how you would handle situations that pose potential ethical dilemmas. The purpose of this is to determine how you, as a 'leader' would deal with difficult situations and lead the team. For example, these questions might focus on how you would handle it if a colleague you were working with decided to withhold information critical to a case as it protects one of their family members, or if one of your employees were dealing with family matters and it was affecting their ability to critically think during an engagement and was impacting their ability to speak to a client. The

question might focus on ‘what do you do’ and expect you to walk the interviewer on what you would say to them and what you would ask them and what you would do in response to what they say.

I am not going to teach you how to be ‘ethical’ or pass these questions because that is just beside the point. However, I would implore you to think logically and give an answer that mirrors your personal values and logic. Most of the time there is no *perfect* answer, there are just bad answers and an incorrect answer. The incorrect answer is obviously the unethical choice. However, how you deal with these scenarios, what you choose to say to the ‘employee’ or ‘colleague’ and how you articulate why you are choosing to say or do what you are going to do, dictate how you perform in this situation. Just remember to think out loud and talk through the process of why you are making the decisions you are making. The point of this is to test your decision making, thinking framework and your personal ethics.

Personal interview questions

These are for the classic interview questions that focus on ‘what is your greatest weakness’ or ‘give me an example where you went above and beyond’. I have always been very honest here and never tried to trick or deceive when I have been asked these interview questions. The reason is, after being on the side of the interviewer and hearing responses like “my weakness is I am a perfectionist” I almost have to hold back the eyeroll. it is so obvious when people are just saying what they think you want to hear or haven’t thought deeply about the weakness. Being a perfectionist is an extremely basic answer it’s like writing a short story and ending it with “I woke up and it was all a dream”. Being a perfectionist is not a weakness. The reason behind why you are a perfectionist is the weakness. For

example, are you a perfectionist because you are insecure about your ability to deliver work that is good enough, or is it for another reason? If so, then just say “I get insecure and feel inadequate, so I check my work and over again”. I am not a psychologist and cannot diagnose this but when asked with these questions, it goes a long way to show some level of self-awareness behind your actions.

We all have a lot of weaknesses and problems. Just pick one that seems to happen the most often. For me, the weakness I have is I have a lot of self-doubt and that stops me sometimes from speaking up or pointing out things. I tend to just assume everyone around me knows more. This is still something I am working on today. Maybe for you, it might be that you are not thorough. This is most certainly the number one weakness I have observed from people around me. Yes, it takes some self-awareness and feedback for people to ‘recognise’ this about yourself – but once you recognise this, you should diagnose if it’s due to lack of knowledge or if it is due to not thinking that much effort is required.

If you stand up in this interview and honestly say that you are not thorough and it’s something you recognise and want to work on, that is not going to result in you not being hired. The point here is honesty goes a long way and it’s not easy to admit your weaknesses. If you do admit them, it creates a strong more trusting relationship between you and your hiring manager as they would respect your honesty.

For questions that focus on giving an example – you don’t need to pull an example from a ‘job experience’ if you don’t have it, it can also be an example from your everyday life in general. The thing to remember here is to make sure that you articulate why the problem was a problem and describe the decision-making process that led to how you responded. If you keep this in mind, I am sure you will do fantastically

Interview red flags

If you are ever asked questions that make you uncomfortable and are too 'personal' and do not seem relevant to the job – for example, if you are married, or if you are going to 'have kids in the future', then call it out. You do not need to respond, and this is certainly 'not normal' behaviour. Politely tell the person interviewing you that you feel uncomfortable and ask the reason why they are asking you the question. I would heavily reconsider working for that company as there are many other companies who would never put you in this position or ask questions like this.

Remember, you have equally as much power as the interviewer, if not more if they have been advertising for this role for a long time. They only have power over you if you choose to give them that power. It is perfectly valid for you to politely decline to answer any question they ask that makes you feel uncomfortable, within reason. For example, if you are interviewing for a threat intelligence role and you get asked a question about whether a hash or an IP is a better indicator, you cannot say you feel uncomfortable to answer this question as this is a perfectly valid question.

Bringing up salary

When researching keywords for this book this was the number one hit for Google searches. Salary. It makes sense. We all want to be paid what we are worth – some people, maybe more. A question I see floated around on Reddit and Quora is the question of 'when do I bring up the salary?'. In answer to this question, often the interviewer will bring this up first. This usually comes up in the first initial call and in the last final interview. They will typically ask you what your expectations are for a salary and maybe

even what you are currently on at your place of work.

Make sure you are aware of what someone with your ‘experience’ and role is getting paid on average. You can even google the salary brackets online for what other people are getting paid. Based on this, you should already have a rough figure of what salary you are looking for from this employer. Do not say something too out of ‘question’. For example, if you are a junior, do not walk into your first job asking for $200,000. It makes no sense and is not aligned with the reality of the industry. When you ask for something extremely high, be prepared for interview questions that match it in difficulty or for the person interviewing you to tell you that it’s outside the bracket for that role.

A good question you should ask is how other people in the same role are being compensated in the organisation. Or you can ask what the salary bracket is for this role. They will usually respond to this. Afterall, it is not fair for you to tell them what you are earning and for them to withhold information about how much the role you’re applying for is being paid. Once you get a gauge of the range, then I would float your offer. Make sure it is not outside of reason. I think the key here is to remember it’s a conversation and just pay attention to their responses to see the feasibility of you getting the salary you want. Most of the time companies are transparent and they will tell you straight up that is too high, or they will say “this can be done”. The interview that follows is what they will use to justify paying you the salary you asked for, or they might come back to you with an offer lower than what you’ve asked for. This might be normalised to match your experience and your technical ability.

Honestly, a lot of different strategies work here. I’ve had friends who straight up asked for the exact salary they want; I’ve had friends who asked for a little bit higher than what they wanted. I have seen all of these normalise to a salary that fits them and their technical skill. Remember, the

people interviewing you have also interviewed for jobs before and are more than aware of the different tactics people use. Whatever you do, just make sure you've done your research and you are aware what your skillset and experience match in salary expectations.

Lastly, don't let companies low ball you and give you an offer far below what you are worth. Ask around, talk to your friends, ask people on LinkedIn what they think about the offer based on your skill. If this company is offering you a fantastic opportunity for growth but can't afford to pay more for your skill, ask yourself if this is a trade-off you are comfortable to make. For me personally, I believe you should always be paid what you are worth and also given opportunities to grow. I strongly believe you can get both from a role and that's what you should aim for too.

Do you like your interviewer?

There's nothing that makes your life more of a hell than working for someone you hate. The interview is a chance for you to see if you like the people you are working with and if you like the manager you are working for. Don't forget that you are assessing them just as much as they are assessing you. So come loaded with questions and make sure that you have enough information to make an informed choice about whether or not you want to work there.

Dress code

During the initial call with the HR representative, recruiter or hiring manager, make sure you ask them what the dress code should be for the interview. Most of the time they will say 'smart casual'. For women, this

can mean pants with a plain t-shirt and a jacket, and for men, this can mean the same thing, or it can mean a shirt with pants. In my honest opinion, I think it matters more how you are 'presented' than the exact garment of clothing you are wearing. For example, if you are wearing pants and a shirt but you look like a mess, you're better off wearing something else. Either way, just make sure you have showered and are clean, and your clothes are clean and that you do not smell bad.

You're being interviewed for your skills and your ability to match the job. However, it's polite to come well-presented and to look like you 'care' about the job. But 'care' does not mean you wear a three-piece suit with a pocket square that makes you look like a realtor with a BMW. It just means come with clean clothes that are work appropriate as if you work there normally, and make sure if it's a video call that you are in an organised quiet room. I have been on an interview call before where a candidate was in a train station with bad reception and came on the call late. This is not a great look.

Common Recruiting Lies

There is a lot of bullshit in cybersecurity. I hate saying this, but it's true. There are lies told by recruiters, consultants who don't know anything about cybersecurity spreading misinformation, and just general lies told to new hires that can affect their overall perception of the field.

If you get told "this is a contract role, but the company is probably willing to extend it to a permanent position" – do not take on any contract roles expecting that you will take on a full-time role at the end of the contract no matter what the recruiter says. Contractors are typically paid higher than normal full-time recruits, just due to the unstable nature of the job. Recruiters often attract people into contract positions as they have a higher

salary – however, if you get extended an offer for a permanent position, this will most likely not be the same level of pay. The other thing to remember is, most of the time these roles do not result in a full-time position.

If you are being sold a dream, it is most likely not going to happen. For example, if you are being paid $80k as a junior and then told that you will be working on hacking cars or breaking into something and that you will be promoted within one year. Do not take the job thinking this means all of this will be a reality when you join the job. Often times recruiters might tell you anecdotes of edge cases or the 'best case scenario' but these are not things that reflect the reality of the job.

If a recruiter tells you that the salary depends on experience and there isn't a set band, they are most likely lying and trying to force you to interview for the role in the hopes you might settle for it. Most companies, if not almost every one of them (outside of fresh start-ups) have defined bands for salaries. The recruiter knows how much the organisation is willing to pay for that role. So if you tell a recruiter how much you are expecting and you ask them how much the organisation is willing to pay and you get told that, chances are you're asking for something outside of the band.

If you have finished your final job interview and you're waiting to hear back and you get told that the company is still interested but are fielding other candidates. This usually means that they are waiting for a better candidate, or that they've sent an offer to another candidate and are waiting to hear back and have you as one of the back-up plans.

If you are told that the working environment is great and that there is no office politics or anything like that in the company, just know it's a blatant lie. It's a part of normal workplace culture where people are competing for promotions and pay rises for there to be a little bit of competition. This will

happen naturally if there are people in different roles with competing agendas. Workplace politics is not always a bad thing.

“You might sometimes have to work overtime, but it’s not that bad”. This usually means you will work overtime. Whether or not it’s ‘that bad’ or ‘good’ should be a decision that you make for yourself given the circumstance. Ask if there is payment for overtime or days in lieu you can take. Always go into these situations with the expectation that you will work overtime and decide for yourself if this is something you are comfortable with.

If you are in a conversation where you feel you are being convinced to take a job, don’t take it. Follow your instinct and don’t try to fit yourself into a shoe that doesn’t fit.

Step 6: Mindset and principles to remember

How well you succeed has a lot to do with your mindset, your decision-making process, what you spend your time on and also how you treat people around you. This last final step are just some tips and things to keep in mind. These are some of the things that have worked for me and the friends around me. You don't need to apply all of these in order to succeed. Find what works for you and develop your own mental framework for how you carry about your life.

Obsession

There is one thing in common between the people that I notice have succeeded in security. It's called obsession. They're fixated on solving a problem and will continuously spend time on it until it is solved. There's no concept of 'giving up' – they enjoy solving the problem and are somewhat 'obsessed' with it. The moment I knew I needed to do cybersecurity was when I was at university and took my first security class. I took that class because I heard it was 'easy' and I was doing easy subjects so I could graduate faster (the humour isn't lost on me). During that subject we learned about what a botnet was and that triggered almost a lifelong obsession that I have to this day. I realised that I get hyper obsessed and focused when I am working on an incident and that 'frame of mind' has really helped me excel. It means that I am willing to go to extra effort just to solve a problem and it means I can't 'finish' something without doing it thoroughly and completely.

With my friends in penetration testing and red teaming, they also tend to be extremely obsessive about their work. When one thing does not work, they

will continuously try more and more things until it does work. Even when something does not seem it will be possible, they refuse to give up. On a penetration testing engagement, my colleague and I were hit with a problem where we could not figure out how to dump out data from an enterprise product that we had gained access to. Instead of moving on and trying to find another entry point, we became particularly obsessed with trying to solve this problem. This ended up in us obsessively trying every possible thing with this product and ultimately resulted in us figuring out how to dump out the database and reverse engineering the encryption protocol used to get the data we wanted out.

If you have no sense of obsession with cybersecurity, does that mean you won't succeed? No. But it does mean that when you're competing with other people in the field who are passionate and obsessive about learning and figuring things out, there is less of a possibility you will be able to outperform them. This does not mean you need to 'force' yourself to be obsessed with something. I think you should just follow your instincts and you might stumble on an area (even if it is not in cybersecurity) that just clicks with you. It's completely bizarre to expect someone who has just finished high school to know what they want to do with the rest of their life. It's not a bad thing to just keep exploring new things and exposing yourself to new industries until you find one that fits.

What's driving you?

I strongly believe that everyone should self-reflect and be really clear on your motivations. Understand why you are doing things and reflect often on how you feel when things don't go a certain way. Do you know why you want to work in cybersecurity? What are you hoping to achieve from a career in cybersecurity? What do you enjoy about cybersecurity? These are

all things you spend time pondering. Take some time to note if your reasons are based on things like prestige, money and/or something less tangible and internal – like passion and fulfillment. Maybe your reasons are a mix of both. Either way, it does not matter too much what your reason is. However, if you are driven by just money, before you waste time jumping into this career – ask yourself, if in 5 years' time there is another career path that makes more money than cybersecurity, would a part of you feel inclined to leave cybersecurity to join that other career path? Also ask yourself, if money was not an issue, is there something else you want to do with your life?

I am a right on the border between Gen Z and a millennial, so my viewpoints on career might be a little different to older generations. I truly believe that with the Internet, people can create a career doing anything that they want if it's what they're passionate about and it's differentiated. For example, Alexandra Botez makes around $100,000 a year playing chess on Twitch, streaming to an audience. There are travel bloggers who make a lot of money to sustain their life and they just travel to places and review them. There are Gen Z people who make money just playing video games online and are 'funny'. There are millionaires who just make videos online about pranking people. I have friends who earn high incomes just selling things they buy from flea markets or making pottery and selling them on social media. There are people out there who run Instagram accounts that just show memes and they sell meme merchandise and make a fortune. The reason I bring this up is because life is too short to force yourself to work in a career just based on money or a superficial reason when you could be doing something you truly feel passionate about. Even if it is not seen as a 'job' by a career standard, it does not mean you cannot make a living from it. It will be the same as any other thing you do in your life – hard, but honestly, you never get far in life when you don't put in effort and work hard as there honestly is no short cut.

I have friends who have gone into cybersecurity for the money and now after a few years working in the field, even over 9 years, I see them quitting. Or they stay and just complain about their job. One of my friends has decided to quit his six-figure job and pursue a job as a gardener for $30k a year.

Not everyone can dedicate their life to a sole pursuit like Jiro and his sushi. This entirely depends on your culture, your personality and your environment and intrinsic motivating factors. It's perfectly fine to start one career, leave and do something else. Everyone moves at a different pace and works things out for themselves at a different pace. The one thing I hope you can take from this section is to make sure you've done some soul searching and have at least some level of awareness of what's driving you to this field. If there is something else calling to you that speaks louder but you're ignoring it for some societal pressure, just be aware of it and consider the choices that you make.

Discrimination

There's no 'one' reason why people discriminate. It can be due to so many reasons – insecurity, fear, ignorance, and so on. Despite all the conversations that are happening about discrimination, racism, sexism – unfortunately, these are all things that still occur even today across several industries. This might come in the form of promotions not being given to you, opportunities not being given to you, or just blatant rudeness and derogatory behaviour in the workplace. This is definitely not normal and there are plenty of workplaces where this is not the norm and is not encouraged. If you are a victim of discrimination, racism or sexism, just remember that you do not need to put up with it. Often times, the people

doing it are not even aware they are doing it and they don't mean it in a bad way.

The only thing I can say here is, don't let it get to you. It's not a 'you' problem, it's a 'them' problem. If something happens that makes you uncomfortable, call it out, and tell someone about it. If you run into a situation where you are feeling uncomfortable, you don't need to suffer in silence. Speak up and report it to your manager or the hiring manager, recruiter or HR representative.

Admitting to mistakes

Everyone makes mistakes. Small ones, monstrous ones; it happens. The worst thing you can do it is try to cover up your mistake. There's one principle that I live by, and that is if you make a mistake admit it openly and honestly. When you lie or try and cover up your mistake, you break trust in the workplace and also with your clients. Even if you make a mistake with the clients, you should admit it openly to them and let them know what has happened. One of my friends told me during a penetration test he accidentally deleted and renamed a lot of files on the client's SharePoint. This was admitted to the client openly and honestly and the client to this date still get work done by this consultant and give him great reviews. I don't think people should ever jeopardise their integrity or character for sake of saving face or losing a job. Most of the time these mistakes that might seem monstrous to you are really not as big of an issue as you might think it is. Be honest and put yourself in the shoes of the other parties. You'd also want to know the truth.

You might not understand things straight away

This is completely normal. When you learn something, there are times when things just do not make any sense. This happens to all of us. Don't let this deter you from learning it. Sometimes the things you learn do not make any sense because you're missing additional context that helps make what you're learning 'useful'. Other times, it might signal that you need to break it up into easier to understand chunks. Either way, there will be a lot of instances where you're exposed to something that makes no sense and it will most likely continue to happen throughout the course of your career.

For me, I remember the first time I felt this was during university when someone showed us how to use Radare2 to reverse engineer a Linux binary. I had no idea what was going on and thought I was listening to another language. I was watching them do the presentation and I honestly had no idea what was going on. I understood at a higher level the purpose and what they were trying to achieve, but I also fundamentally did not understand how they were doing it and how to do it myself.

I tried to learn how to reverse engineer by reading some books and some simple tutorials. However, there was a massive steep learning curve ahead of me. It is not easy and even now, I definitely do not think it's easy. It takes a lot of time, effort, practice and a lot of mistakes. The feeling of learning something new and being overwhelmed by how much you need to learn is completely natural. It means you're being pushed outside of your comfort zone. This is a feeling you should try to seek and get used to. It's a mental muscle that you're learning how to use and control, the more you do it and put yourself in situations that stretch you, the easier it will become.

Experienced Hires: ‘I don’t want to start again’

This is something I hear a lot from people who want to transition to a new career path or even an adjacent career path like IT to security. It’s the ‘I don’t want to start again’. Maybe you’ve worked a few years in your current position and you’re comfortable on your current salary, but you’re struggling to make the transition into cybersecurity because you don’t want to start at the bottom again as an analyst.

I have some good and bad news. For people in IT who already have job experience, it’s not as difficult for you to transition into cybersecurity and maintain some similar to where you’re at as the fields are related to each other. For people in a completely different field for example, medicine, it might be a little more difficult.

The bad news is you will be paid completely proportional to how much knowledge and value you will bring to the organisation you are being hired for. If you are an experienced IT person but are struggling to connect the dots to cybersecurity and lack experience in a security setting, you will not be paid as well as someone who does have that capability. For people in medicine or a different field, you are going to have to accept the reality that you will be competing with other people who are already in the security field with experience. You will either have to start from the bottom again or you are going to have to find a way to stand out and show that you have the experience that is required even though it’s not necessarily in the form of a ‘prior job’. This can be done through digital proof of your experience as mentioned in the earlier steps in this book. If you are a Senior Marketing Executive, looking to be a Senior Penetration Tester with no proof of your skills on your resume, you are most likely not going to land even an interview. This is just the reality. Other candidates will be chosen above you who have the proof that they have the skills.

When I was at University, I was also working as a Digital Executive in a marketing firm. My job centred on web development for clients, programmatic advertising and content marketing. I wanted to transition to cybersecurity, and I knew it would come at a salary cut as I had no experience whatsoever. I landed a job as an analyst with the same salary, and it was due to my blog and the other things I had done that were security related – i.e. winning awards in CTFs I had competed in at a national level and other things I did in my spare time. This is just a band-aid that you will unfortunately have to rip off. If this is the career you want to go into, I personally would just cut your losses and make the transition sooner rather than later.

Dealing with that 'Technical' person

There are technical people who are nice and humble, and then there are the 'technical' people – or that 'technical guy' who might not be so nice and humble. They are in-your-face about their skills and want to demonstrate that they are more technical than you. I am bringing this up because almost all of the people around me have dealt with someone who is this 'technical' persons. This is someone who you might come across at some point in your career and this is what you should be aware of.

Who is that 'technical' person? That 'technical' person is the kind of person who likes to flaunt their technical knowledge and let you know that they are more technical than you. They do this to separate themselves from you – you in the 'untechnical' bucket, and them in the 'technical' bucket. They are usually always at conferences, security events and they are either talking to the presenters, presenting, standing alone or have a crowd of people around them. Typically, you will run into this person if you work in an area of

security that prides itself on technical knowledge – for example incident response, penetration testing / red teaming and or malware analysis / reverse engineering.

The way that ‘technical’ person separates themselves from you or lets you know you are not as ‘technical’ as them can happen in many ways. This might occur in the form of them asking you some obscure question, and then proceeding to tell you the answer and playing it off as if they are ‘educating’ you. Or they might just be extremely direct and tell you that you’re not technical and point out areas where you are lacking in knowledge. Sometimes this person might point out mistakes you’ve made or penalise you for asking questions that might seem ‘untechnical’ or ‘stupid’. This might be done with an audience watching. Some of my friends describe talking to people like this as an ‘excruciating experience’. The reason is, most of the time the conversation will centre on them, their achievements, what they’re working on, the things that they have researched, and they might go into extreme detail on something extremely niche to demonstrate their ‘technicality’ to you. This might then end with them asking about what you’ve done and then ‘subtly’ trying to ‘educate you’ on how they would’ve approached what you did in a ‘more technical’ and ‘better’ way.

Usually that ‘technical’ guy might be someone who is just socially challenged but actually means well. Sometimes, they are not socially challenged and do not mean well. The difference between these people lies in their intent. Working out the intent becomes extremely obvious when you are in this situation talking to that ‘technical’ guy. You will know.

There are many ways of dealing with that ‘technical’ guy. The first one is to recognise that they are essentially putting on a ‘show’ for you or for others to create an image that they are ‘more technical’ to gain clout or respect. This can be due to insecurity, a need to control their ‘image’ or just sheer

ignorance and arrogance. The second is to make a decision if you want to continue speaking with them, or not. If you do not want to speak with them, then find a way to politely excuse yourself from the conversation. If you do want to continue speaking to them (perhaps if you are in a group setting), then just remember that this kind of person tends to get triggered if you 'question' their knowledge, 'question' their conclusions or anything that they have done as this might impact their 'public perception' as the most technical person there. If you're interested in what they are saying and want to learn more about it, then this is the perfect person to ask questions from. These people tend to be extremely open and wanting to share their knowledge because it reinforces to them that they are 'technical' and you asking questions is a 'recognition' of that. Personally, for me, I do not mind engaging in conversations with people like this. The reason is because I am used to it coming from a computer science background and I find that if you start asking them questions or show interest in what they're saying they tend to stop 'demonstrating' their knowledge to you and can speak more naturally. If you do not want to speak to them but are stuck with them in a group, I would just encourage letting that person finish speaking and then politely divert the attention to someone else in the group with a question.

Either way, it's just always a good habit to not take things too personally. Don't let it bother you and don't let it make you feel bad about knowing things. Everyone moves at a different pace and everyone knew nothing at one point. With this, I just want to add that the lesson you can take from this is just to be respectful, mindful and humble. Just because you know more than somebody right now, does not make you better than that person. If that person was equipped with your knowledge, they might excel past what you have achieved in a shorter time. How much someone knows and how much better they are, are not directly correlated means of measuring someone's 'worth' in a field. Treat people the way you want to be treated and remember that when you are an asshole, people will remember it and it will impact your reputation.

Social Skills

Cybersecurity attracts a lot of introverts. However, if you want to move up the corporate ‘food chain’ and get paid more money, it becomes more and more important to become well-rounded and to have developed the communication skills to socialise and articulate your points. There are many technical people who struggle with communicating what they have done, how they did it and why it is important. There are people who are not technical who can communicate very well. The people who end up rising up to the top tend to have a mix of both. They do not need to be the most technical person, nor do they need to be the most excellent communicator, but they do need to be well rounded and have good interpersonal skills. If you happen to be excellent at both of them, then you will no doubt excel. There are many senior jobs where no matter how technical you are, if you struggle with communication, you will not land the job. It’s just something to consider, and a skill that in my opinion is always worth learning.

Social skills are not something you are naturally born with. Even though some people might just seem more ‘socially’ fluent, it has more to do with exposure to situations at an early age. Just like everything else, it is a skill that can be acquired. It just takes time, and it takes practice. There are a lot of benefits to having good interpersonal skills that stretch far beyond just work-place benefits. If this is something that you want to develop, then I would suggest just try attending more industry events, try to meet new people and strike up conversations.

Onwards and upwards

Thank you for choosing to read this book. I hope you have taken something away from it and that it helps you achieve your goals in cybersecurity. These are just the things that I have picked up along the way which have helped me get to where I am. With perseverance, determination, passion and hard work, you will get to where you want to be in the industry. I hope that when you do, you can find some time to give back and help others along the way too.