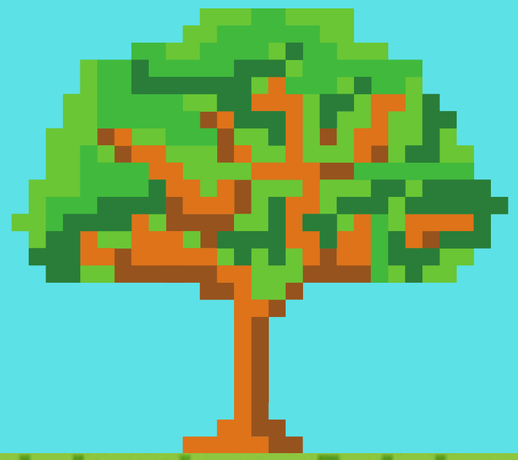
LEVEL UP
A CAREER IN SECURITY

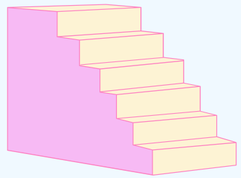


START

MENU

1. CAREERS IN SECURITY

2. GETTING STARTED



3. PERSONAL BRANDING

4. JOB HUNTING

5. MENTAL GAME

6. RESOURCES

CHARACTER SELECT

HP

MP

CLASS NETRUNNER

ABILITIES

GABRIEL MATHENGE | AKA V1V1

- Security enthusiast.
- Offensive security and other things.
- Hiking, running, gaming, watching CSGO.

Twitter: https://twitter.com/_theVIVI

Blog: https://thevivi.net

GitHub: https://github.com/V1V1

Discord: V1V1#0804

Email: gabriel<at>thevivi.net

BEFORE WE GET STARTED...

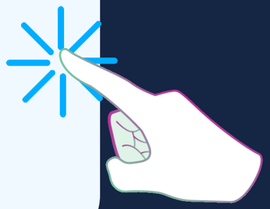
1. Opinions are heavily biased by my personal experience.

2. Been on both sides of the interviewing table.

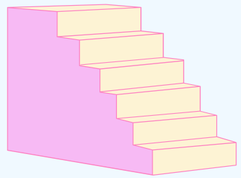
3. I've primarily worked in offensive security, but I'll generalize as much as I can (focus on technical roles).

MENU

1. CAREERS IN SECURITY



2. GETTING STARTED



3. PERSONAL BRANDING

4. JOB HUNTING

5. MENTAL GAME

6. RESOURCES

CAREERS IN SECURITY

- There are A LOT of career paths in cybersecurity.
- This is both a **good thing** (lots of opportunities) and a **bad thing** (choice overload - especially for beginners).

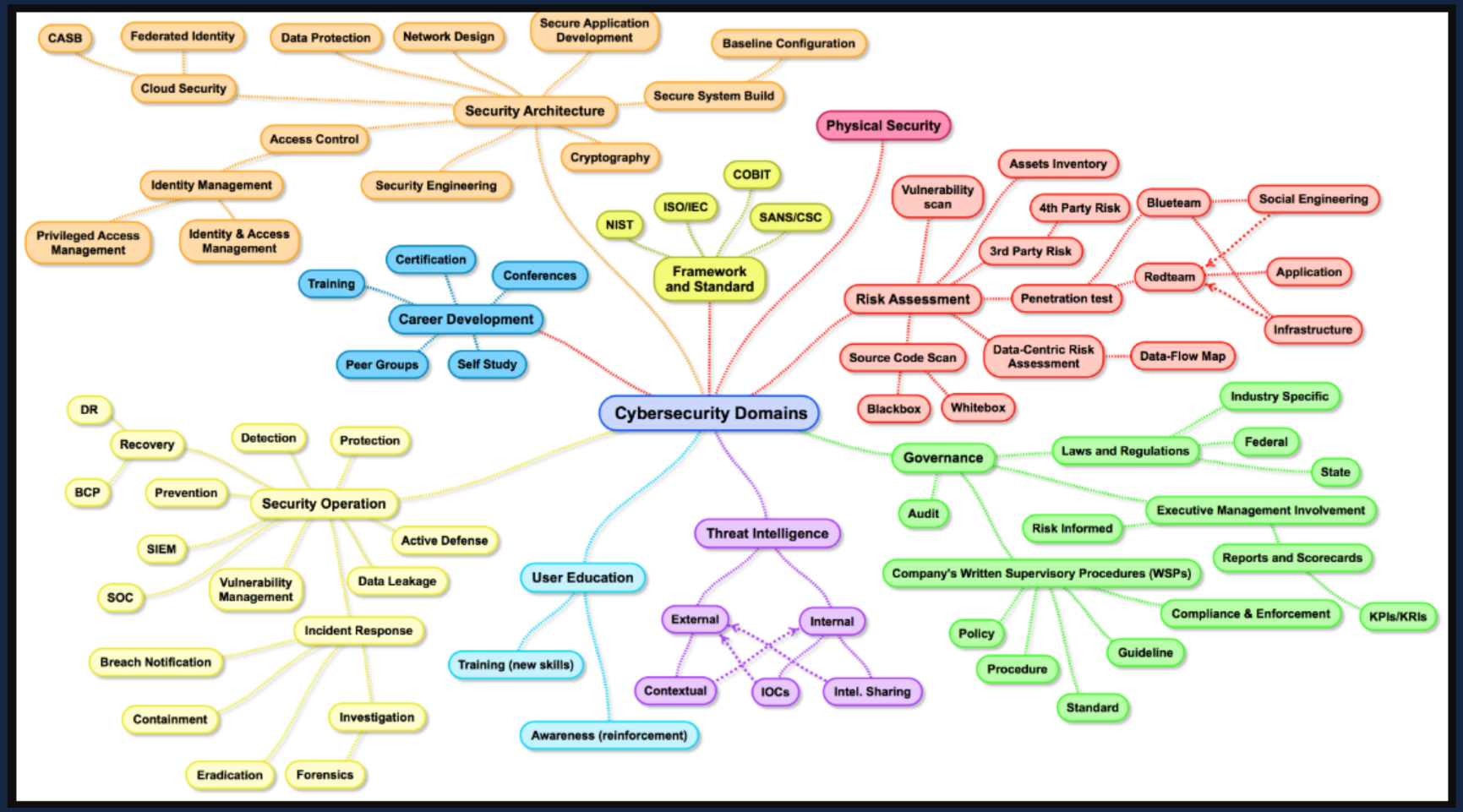
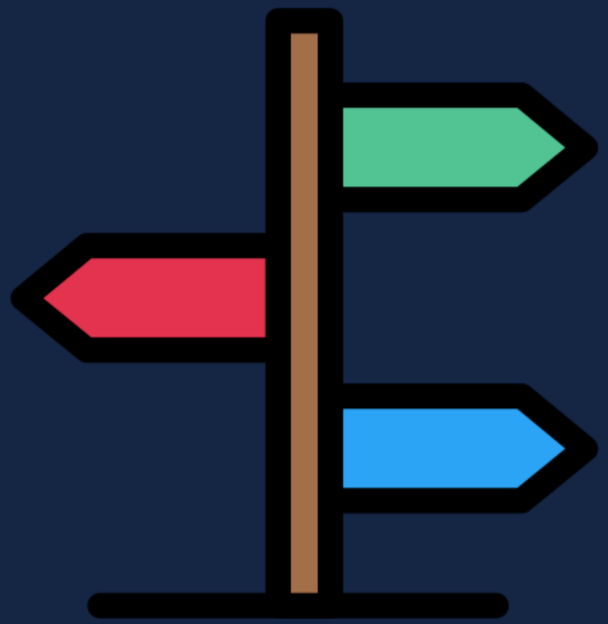


Image source: https://cybersecurity.att.com/blogs/security-essentials/theres-no-such-thing-as-an-entry-level-job-in-cybersecurity

INTERNAL VS EXTERNAL

- I'm generalizing a lot here, but you can typically get security work in 2 general forms:
  - As part of an organization's **internal security team/department**.
  - As an **external resource** offering security services to other organizations e.g. consultant doing incidence response, managed SOC, pentesting etc.

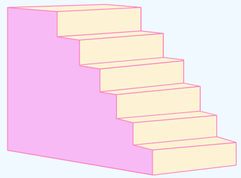


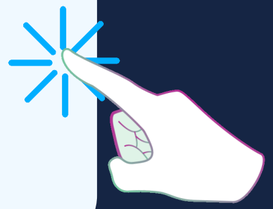
- In an internal team, the vast majority of the work you do will be focused in your **employer's environment** (apps, infra, policy, research, people etc)
- As an external consultant, you'll be doing **work for other organizations** (a.k.a clients) to make money for your employers.
- Both have their advantages and disadvantages. Your choice here will be influenced by your personal preferences and available opportunities.

MENU

1. CAREERS IN SECURITY

2. GETTING STARTED





3. PERSONAL BRANDING

4. JOB HUNTING

5. MENTAL GAME

6. RESOURCES

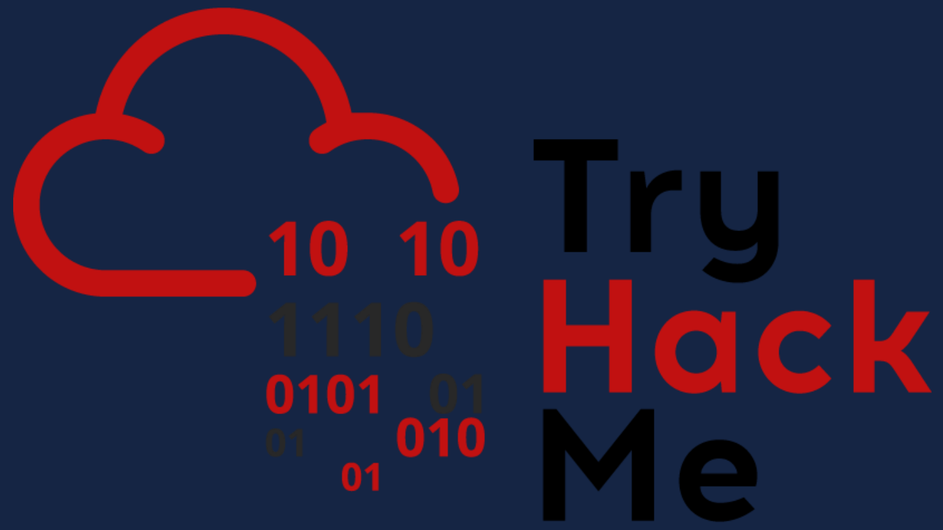
WHERE DO I EVEN START?

- If you're feeling a little too overwhelmed to begin with, then don't be afraid to **be flexible and a bit of a generalist** at the beginning.
- Security is a field that incorporates a lot of other IT domains; system administration, networking, coding/scripting etc.

- You can start by learning some of the basic skills required in a ton of technical roles:
  - **Operating systems** - get familiar with Windows & Linux OSs. Especially using the command line.
  - **Coding/scripting** - learn a popular scripting language (Python, Go, Bash, PowerShell, etc.)
  - **Build a home lab** - with whatever you want in it. Just do it.
  - **IT/security concepts/frameworks** - CIA triad, attack kill chain, popular protocols, security frameworks e.g. NIST, MITRE ATT&CK.
- These general skills will be a bonus regardless of whatever path you choose to go down later in your career.

TRYHACKME

- TryHackMe is an incredible resource for beginners because of its learning paths. **$10 a month** is a lot cheaper than paying for a cert.
  - *https://tryhackme.com/paths*
- Complete beginners can start from some of the **basic learning paths** and diversify from there:
  - *https://tryhackme.com/path/outline/presecurity*
  - *https://tryhackme.com/path/outline/beginner*
  - *https://tryhackme.com/path/outline/introtocyber*
- These beginner paths are great for building a **solid foundation** that you can then add to with more complex topics.



- Don't lock yourself into a single field/set of subjects, especially when you're just getting started:
  - "I want to be a pentester so I'll only learn offsec topics".
- Defense complements attack and vice versa.

FOCUS ON WHAT EXCITES YOU

- After trying out different things, you might find a few subjects that you **enjoy doing more than the others**.
- At this point, you can focus on learning more about those specific subjects e.g. digital forensics, vulnerability research, malware analysis, CTFs.
- Do your googling, look for free content/courses in those specific areas.
- Hunt for **content creators** that focus on these fields.
- Look for **awesome-[insert-subject-here]** repositories on GitHub:
  - *https://github.com/0x4D31/awesome-threat-detection*
  - *https://github.com/rshipp/awesome-malware-analysis*
  - *https://github.com/yeyintminthuhtut/Awesome-Red-Teaming*
  - *https://github.com/FabioBaroni/awesome-exploit-development*
- These are usually great repos with additional resources for specific topics.

- **NOTE:** Don't worry if you don't find your "passion", just keep learning until you find something that you don't hate doing. Focus on **consistent growth**, you don't always have to know where you're going. The "useless" things you learn now could create value later in your future.

WHAT DO YOU PREFER?

- **RED PILL** - Deep dive and be an expert in a specific topic.
- **BLUE PILL** - Be a generalist, competent at a much wider variety of subjects.

THE NOT-SO-PAINFUL TRUTH

- There is **no right answer** here.
  - Some people get incredible success by being very, very good in a specific field.
  - Others earn their success by being generalists.

- Because of the nature of my work (pentesting/red teaming) and the dynamism of the technological landscape, my personal preference is being competent at a wide variety of topics and much better at a few specific ones.
- **NOBODY** is an expert at everything.
- Once you're working with others, you'll learn that different people's strengths is what a makes a great team.

EDUCATION & CERTIFICATION

- A lot of big corporates still list a degree as a minimum requirement.
- Other firms may be more flexible with their policies. This varies a lot, so there's no standard.
- What matters is that you know that **you can make it** infosec regardless of your background.

- As for certifications, you tend to see some of the same ones being listed for the job you're looking for e.g. for offensive security work you'll tend to see:
  - OSCP
  - CEH
  - Security+
  - CRTP/CRTE
- Other really popular ones in job ads:
  - CISSP
  - Cloud certs (Azure, AWS, GCP).

CERTS ON THE CHEAP

- You may not have the resources to get $1500 certs at the start of your career. But that doesn't mean you can't do something about it.
  - Offers on sites like Udemy (finish the course, get a cert):
    - *https://www.udemy.com/*
  - TryHackMe - course completion badges:
    - *https://tryhackme.com/*
  - Microsoft learning paths & training days (free Azure cert attempt!)
    - *https://www.microsoft.com/en-us/trainingdays*
    - *https://docs.microsoft.com/en-us/certifications/exams/az-900*
  - AWS cloud training
    - *https://aws.amazon.com/training/*
- Stay on the lookout for free/cheap certification opportunities.
- Make the most of them. Do as many as you can while you've still got the time.

TAKE DETAILED NOTES!

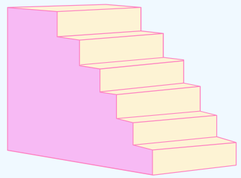
- One of my biggest regrets is that I didn't start taking detailed notes earlier in my career.
- Note-taking is probably the most important skill for security professionals.

- You'll be learning a lot...constantly. Nobody can remember everything they read.
- You don't want to end up in a position where you're relearning a topic you've already touched before.
- So pick a note taking app and start recording the things you learn. It's a game changer, just trust me:
  - **EverNote** - *https://evernote.com/*
  - **OneNote** - *https://www.onenote.com/*
  - **Obsidian** - *https://obsidian.md/*
  - **Notion** - *https://www.notion.so/*
  - **CherryTree** - *https://www.giuspen.net/cherrytree/*

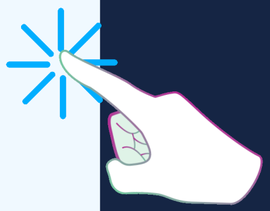
MENU

1. CAREERS IN SECURITY

2. GETTING STARTED



3. PERSONAL BRANDING



4. JOB HUNTING

5. MENTAL GAME

6. RESOURCES

BE SEEN

- Another one of my big regrets.
- Start working on your brand at the beginning of your career.
- With the hyper-connectivity of today's world, it's a lot simpler to do than it's ever been.

- What do people find when they look you up?
  - It's **not about being famous**, or having 10,000 followers.
  - It's about making it easier for others to **find out what you're all about**. Your work, your research, skills, experience, interests, etc.
  - It's also about **connecting with others** that share your interests.

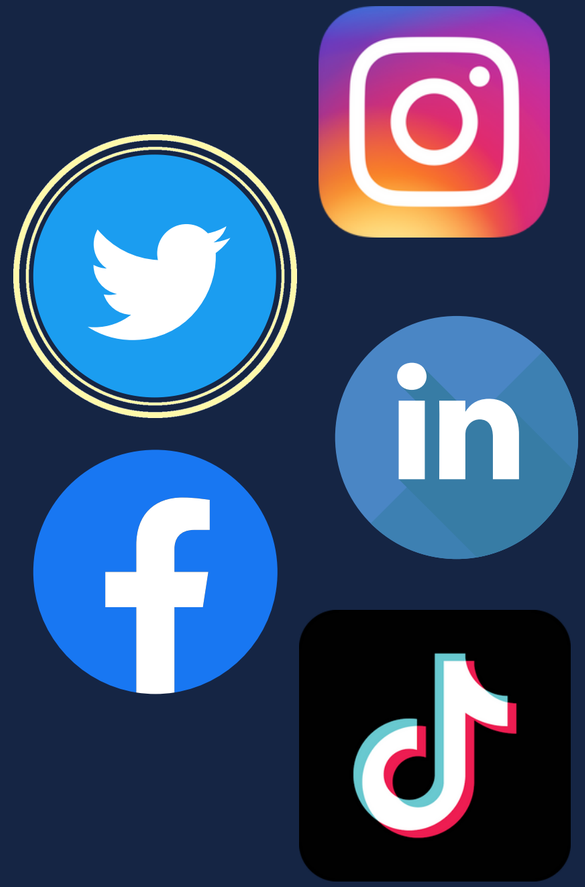
- For most of us, **it takes a long time** to start "being noticed".
- The earlier you start, the easier it will be for future you to add to your brand.

SOCIAL MEDIA

- I'm not here to convince anyone to join social media.
- If you're living a happy life without it, then carry on.

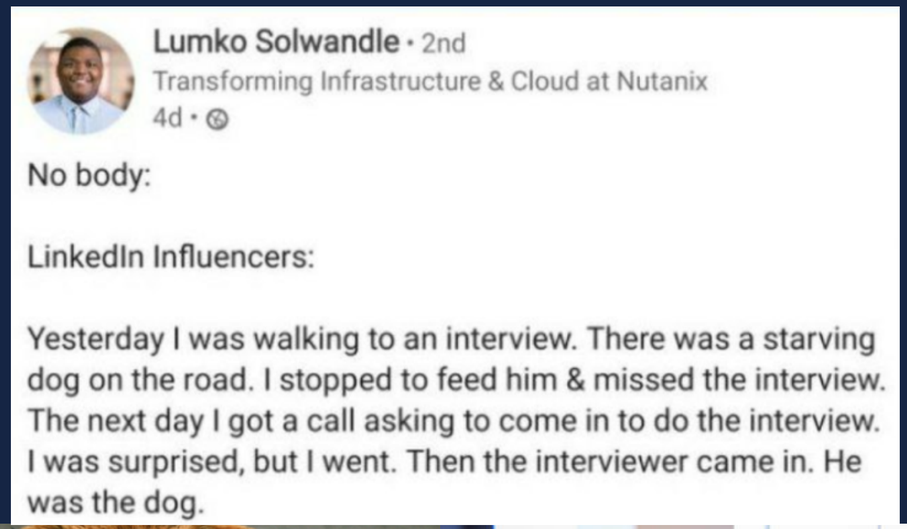
- But if you do want to start connecting with professionals in your field, then you really should consider joining Twitter.
  - *https://twitter.com/*
- Infosec folk (and a lot of other techies) primarily hang out on Twitter.

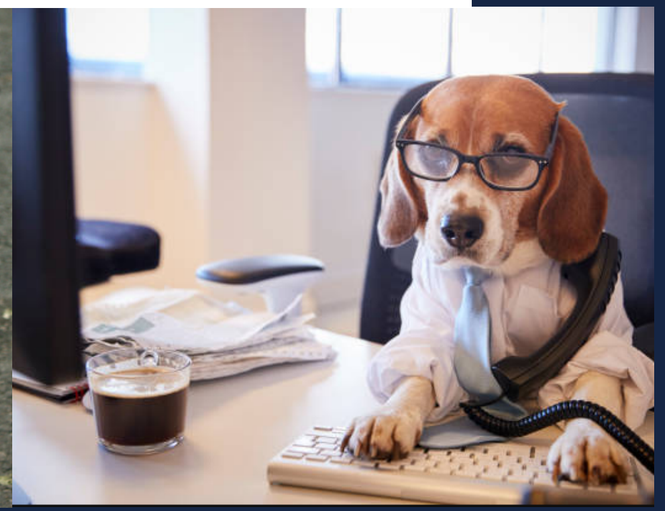
- Start by following a few local and international people in your field of interest.
- Get used to sharing your **progress/achievements**. Even if it feels lame compared to the stuff you're seeing online.
- We all start from zero.
- **Sad fact:** the impostor syndrome from social media never gets any less intense, you just get better at dealing with it.



LINKEDIN

- The site everybody loves to hate. Including myself.
  - https://www.linkedin.com/feed/
- **LinkedIn = 85% ridiculous "inspirational" stories + 10% jobs you'll never get + 5% jobs you might get**





A NECESSARY EVIL

- As much as I hate the site, it's one of those "**better to have it and not need it than to need it and not have it**" type of situations.
- LinkedIn is useful for personal branding in the professional world.
- Why?
  - **Twitter** = infosec & other techies.
  - **LinkedIn** = HR & recruiters.

- You'll probably be at a disadvantage when applying for jobs early in your career if you don't have a profile.

- Share your **achievements** (certifications, courses), **public content** (blogs, tools, presentations).
- **Connect** with others in your field.
- Believe it or not, it is actually possible to get a job using LinkedIn.

CONTENT CREATION

- One of the best ways to impress your peers is to **create content**.
- Content can come in all manner of flavors:
  - **Blogging**
  - **Videos** (YouTube/Twitch)
  - **Presentations**
  - **Tooling** (GitHub)
- Play to your strengths. If you don't like the sound of your own voice (who ever does?) then write a blog. If you don't like writing, then record a video or develop a tool. There are tons of free options these days. Use them.

zoom

REMEMBER!

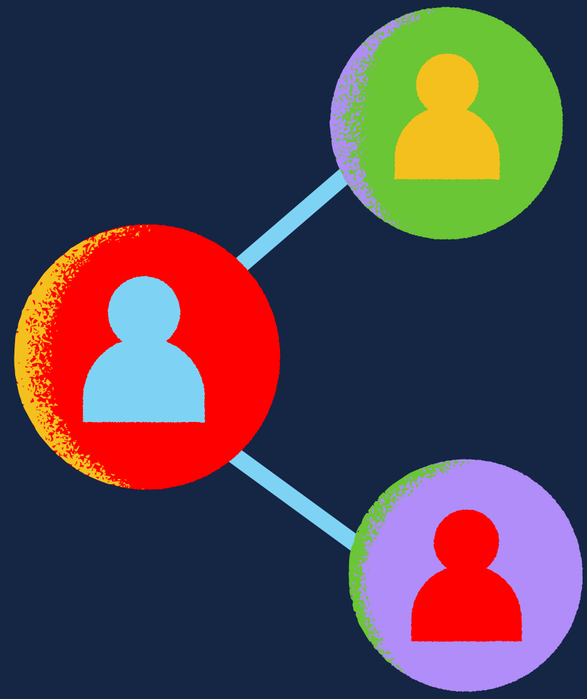
- Don't hold off on content creation because "you're not ready yet".
- You'll NEVER be ready and you'll never get good unless you're bad first.
- So what if your content is beginner level/basic?*
- So what if there are already 200 blogs/videos about that topic?
- You have value. Somebody out there wants to see your content.
- Everybody has something worth sharing.

* - the most popular type of content on the internet tends to be the stuff made for beginners.

NETWORKING

- A good network is worth its weight in gold.
- Sometimes it's not what you know, but **who you know**.
- A big part of your brand is how far it spreads - the bigger your network, the wider your reach.

- People want to work with their friends - or with people they're familiar with or have at least heard of.
- A significant number of jobs are advertised as formalities. A lot of the time, the candidates they're actually considering are people from the current team's networks.
- Your network (combined with everything else) will help you **stand out from the crowd**.
- Networking isn't easy for everyone (I personally struggle), but its value can't be overstated.



CONNECTING WITH OTHERS

Twitter

Conferences

Discord

Courses/cert channels (e.g. on Discord)

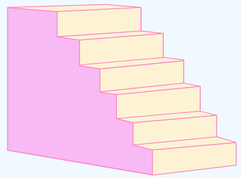
People reaching out to you because of content you created

yeah...this too

MENU

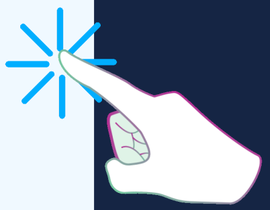
1. CAREERS IN SECURITY

2. GETTING STARTED



3. PERSONAL BRANDING

4. JOB HUNTING



5. MENTAL GAME

6. RESOURCES

CV

- Your CV's purpose is to advertise the best part of you to employers.
- Everything in it should help you. Leave out anything that doesn't.
- Invest a lot of time in the beginning; building a resume you like and that's easy to edit when you need to.
- Research **ATS (applicant tracking system)** compliant CVs:
  - *https://www.topresume.com/career-advice/what-is-an-ats-resume*
  - *https://zety.com/blog/ats-resume*

- The best advice I can give here is to tailor your CV to the job you're targeting.
- This is an exhausting process that you probably can't do for every single application, but if it's a job you're truly invested in getting then tailor your CV to match the job's requirements.
- **Tailoring?**
  - Editing key areas of your CV to match the job requirements.
  - Key areas: experience, skills, achievements, tools you're familiar with, industries worked in etc.
  - Use the JD or job ad as a guide for what to include.

CV FORMAT

- The format you use is completely up to you.
- The length is also a personal choice, but don't be extreme.
- HR/recruiters are people just like you. Nobody wants to sit down and read a boring novel about your life.
- My personal preference is 2-3 pages (depending on experience). Could be less, could be *slightly* more.

Meg West, CISSP

Blahblahblah@Gmail.com | +1 000 000 0000 | in https://www.linkedin.com/in/cybersecmeg/
https://twitter.com/cybersecmeg https://www.youtube.com/c/CybersecurityMeg

Objective: *To utilize my extensive incident response, team leadership skills, and threat hunting capabilities to assist in keeping organization's names out of the evening news.*

Certifications

- (ISC)² Certified Information Systems Security Professional (CISSP) – September, 2020 (Certification Number: 000000)
- CompTIA Security+ – June, 2020 (Candidate ID: COMP000000000000)

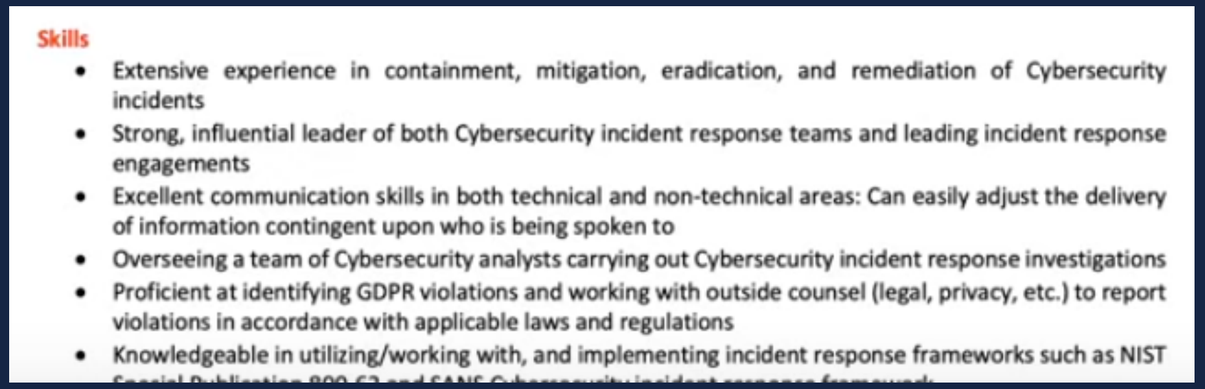
Education

- Master of Science in Cybersecurity – Earned August, 2019
- Bachelor of Science in Political Science – Earned August, 2017

Experience

Global Cybersecurity Incident Response Manager – Tech Data Corporation, October 2020 – May, 2021

I am responsible for overseeing all incident response initiatives at Tech Data (a Fortune Top 100 company with revenue exceeding $30 Billion USD a year). Since beginning in this position, I have greatly reduced the time it takes for *insert what you have improved here*. I have mentored the Cybersecurity analysts to assist in advancing their skillsets and knowledge of incident response. I constructed a new procedure from the ground-up wherein *insert beneficial change that happened here* which allows *insert the result of the beneficial change that was made*



Skills

- Extensive experience in containment, mitigation, eradication, and remediation of Cybersecurity incidents
- Strong, influential leader of both Cybersecurity incident response teams and leading incident response engagements
- Excellent communication skills in both technical and non-technical areas: Can easily adjust the delivery of information contingent upon who is being spoken to
- Overseeing a team of Cybersecurity analysts carrying out Cybersecurity incident response investigations
- Proficient at identifying GDPR violations and working with outside counsel (legal, privacy, etc.) to report violations in accordance with applicable laws and regulations
- Knowledgeable in utilizing/working with, and implementing incident response frameworks such as NIST

Public Speaking/Recent Cybersecurity Community Involvement

- (ISC)² Global Diversity, Equity, and Inclusion Task Force Member (March, 2021 – June, 2022)
- (ISC)² International Women's Day Panelist Speaker (March, 2021)
- Leader of Certification Station Cybersecurity Prep Group (10,000+ global members)
- Leader of InfoSec Prep Cybersecurity Group (19,000+ global members)
- University of South Florida Cybersecurity Career Mentor (2018 – Current)
- Apple Cybersecurity Awareness Podcast Host (January, 2021)
- Recorded Future Predict Conference Speaker (October, 2020)
- SAP ASUG (America's SAP User Group) Speaker (June, 2020)
- SAP Sapphire Now Selected Speaker (April, 2020)

Articles/Presentations/Interviews

- https://www.youtube.com/watch?v=e0wUt7QEKs0&t=99s
- https://www.youtube.com/watch?v=WcbQamin3Cc&t=3s
- https://securitytrails.com/blog/interview-cybersecmeg

Watch this video: *https://www.youtube.com/watch?v=Y4YUWWI8LPY*

THE TYPICAL INFOSEC JOB AD

BASIC REQUIREMENTS

- Doctorate in Computer Science or related field.
- 5+ years of experience in multiple security disciplines (red teaming, blue teaming, purple teaming, rainbow teaming, exploit development, beatboxing).
- 4+ years of leadership experience - preferably at a C-suite level.
- Knowledgeable in at least 8 programming languages.
- Minimum certifications - CISSP, OSCP, OSCE3. CRTO, CRTO II, PACES, CRTE

JOB LEVEL

- Entry level.

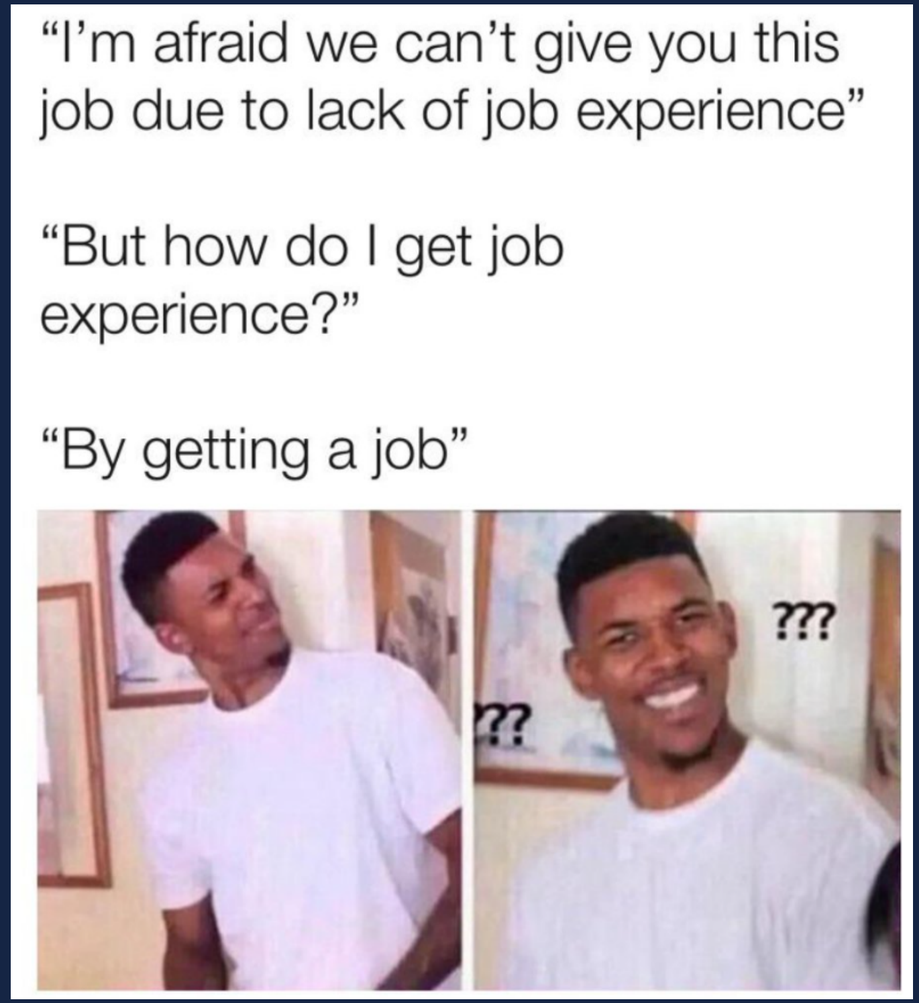
SALARY RANGE

- I hope you like being broke in the second week of the month.

If employers were honest about what they're looking to hire.

APPLY ANYWAY

- You may have heard this before:
  - "there are no entry level jobs in infosec"
- I don't agree, but it's true that employers are notorious for advertising infosec job roles with **insane requirements** for entry level candidates.
- It never gets any better, a lot of senior roles also have unrealistic demands/expectations.



What I've learned?

- Some employers are looking for a single infosec resource to solve ALL of their security problems.
- Don't let job requirements scare you off. **Apply anyway**.
- Do your best to meet the **most important requirements** - these are usually pretty obvious (e.g. a cloud security engineer should probably know a lot about cloud security).
- Have confidence in your **ability to learn new skills**. We're all learning on the job.

EXPERIENCE BEFORE EXPERIENCE

- So how do you show experience before you actually have any?
  - Completed any **courses or certs** - Make use of those course completion badges/certificates. Add them to your CV.
  - **Profiles** on TryHackMe, Hack the Box, GitHub?
  - **Content creation** - Blog? YouTube channel? Podcast?
  - **Member of a community** e.g. BSides/SheHacks/AfricaHackon.
  - Part of a **CTF team**? Competed in any tournaments?
  - Add a **projects** section to your CV:
    - Home lab? Built an AD environment?
    - Sign up for free cloud credits (AWS, Azure) - try do a project on it. Document it somewhere, add it to your CV.
    - Volunteered to do anything in the community?

- Watch this:
  - https://www.youtube.com/watch?v=wwiPnpmYqIk&t=22s

STAND OUT

- The point here is **stand out from the crowd**.
- If all 10 of the final candidates have a degree, the same certs, the same years of experience - then it's **the little things** that will make a difference.
- Personal projects, community contributions, content creation and so on.
- They might not seem like much initially, but these little things add up.

WHERE TO FIND JOBS?

Network

LinkedIn

Recruiters

Don't be afraid to go global

(relocate/remote work)

PREPPING FOR AN INTERVIEW

- The most important thing you can do for interview preparation is to **research the hell out of the company**.
  - What's their interview procedure?
  - How many stages?
  - Is there a technical challenge/CTF?
  - Common interview questions?
- Do you have a connect there?
  - If you know someone that was or is a part of the company, then use that relationship to get as much insider info as you can.
  - Don't ask for technical challenge solutions or anything that incriminating - you still want to earn the job.
  - Just find out what prep you can do to ace the interview.

- Sites like **Glassdoor** are pretty great for learning about the interview process:
  - *https://www.glassdoor.com/index.htm*

EXAMPLE INTERVIEW PROCESS

Phone screening

Technical challenge

Interviews with the team and/or leadership

Financial negotiation

Onboarding

SITUATIONAL QUESTIONS

- A lot of organizations use **behavioral interview questions or scenarios**:
  - What would you do if you were places in situation X?
  - Describe a time when...
  - Share an example of a situation where...

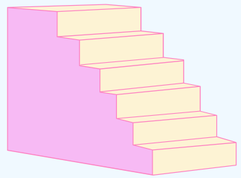
- Learn about these types of questions and scenarios from Glassdoor and how to answer them.
- The **STAR (Situation, Task, Action, Result)** method is a great technique for this:
  - *https://www.thebalancecareers.com/what-is-the-star-interview-response-technique-2061629*
  - *https://www.thebalancecareers.com/competency-based-interview-questions-2061195*

- **NOTE:** Interviewing is a skill like any other, the more you do it - the better you get at it.

MENU

1. CAREERS IN SECURITY

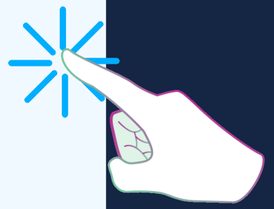
2. GETTING STARTED



3. PERSONAL BRANDING

4. JOB HUNTING

5. MENTAL GAME



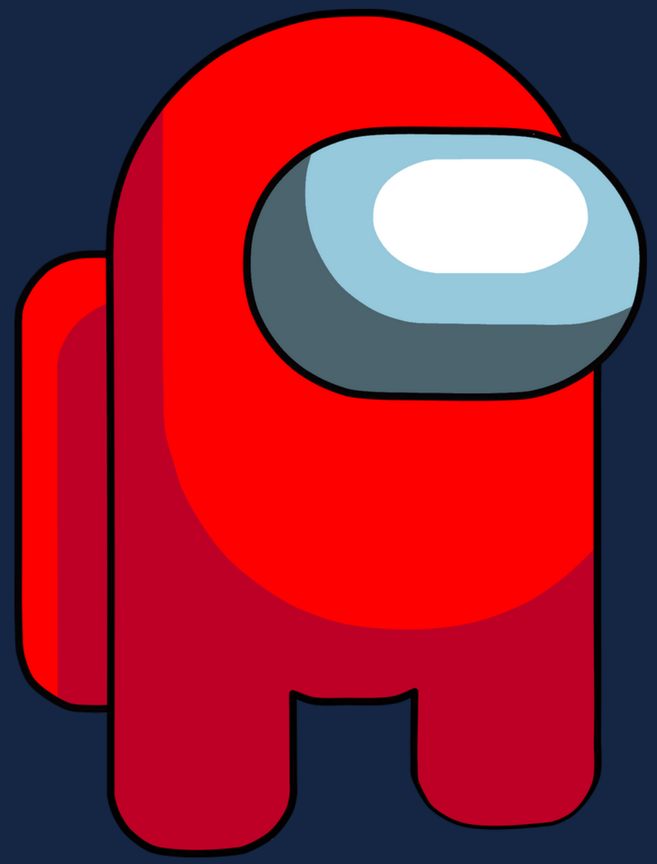
6. RESOURCES

IMPOSTER SYNDROME

- This is almost always a constant. **Social media** makes it worse.
- **Everyone online is always winning**, doing cool security things while you sit around and think about how incompetent you are.

- I'd love to say it stops, but it never really does (at least not for me).
- **You're not alone** though - a lot of people feel it.

- How to deal with it varies from person to person, but the crucial thing is **not to let the feeling stop you** from putting yourself and your work out there.
- Even if you feel like an imposter; publish that blog, sign up for that cert, apply for that job or whatever it is you're dreaming about.
- If this demon is gonna follow you around forever, might as well **do the stuff you want to do** anyway ¯_(ツ)_/¯



BURNOUT

- Infosec can often be a very demanding job.
  - "Find a job you're passionate about and you'll never have to work a day in your life".
- **This is garbage**. Work is work - and work sometimes sucks.

- Passion & motivation run out. Sometimes all you'll want to do is quit.
- The longer you stay in a field, the easier it is to burnout.

- Learn to **identify the symptoms** and figure out a solution that works for you. Meditation, social activities, exercise, gaming - there are a lot of options.

- Find hobbies that get you a way from the grind for a while.
- Use them to recharge your battery before diving back into the mess again.

TAKEAWAYS

Everyone's experience is different

Learn from others but write your own story

Every single job has crappy parts to it

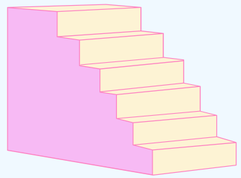
You can learn from any situation

The only real enemy is complacency

MENU

1. CAREERS IN SECURITY

2. GETTING STARTED



3. PERSONAL BRANDING

4. JOB HUNTING

5. MENTAL GAME

6. RESOURCES

RESOURCES

Career Guides

- https://c3rb3ru5d3d53c.github.io/personal-blog/2022-06-21-a-career-from-nothing/
- https://www.hexacorn.com/blog/2022/08/19/what-to-know-what-to-learn-what-are-useful-skills-for-cyber-in-2022/
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/want-to-become-a-red-teamer-this-is-what-you-need-to-know/
- https://blog.pentesterlab.com/a-strategy-to-land-your-first-pentest-job-25209a351689
- https://twitter.com/varcharr/status/1488930419768758277?t=c_-mjWzPGBWIXO4gcuNB-w&s=09
- https://twitter.com/GrahamHelton3/status/1569004212364640260?t=gwqhSmCHWSzEyNdbiSw2iQ&s=35

Job hunting

- https://www.jhaddix.com/post/a-hackers-guide-to-finding-cybersecurity-jobs
- https://medium.com/@0xP/offensive-security-getting-your-foothold-in-the-industry-ac0267cf77a0
- https://twitter.com/nullenc0de/status/1560639105767440386?t=flym5Y2eC4ASjyA-bA76Hw&s=35

Videos

- https://www.youtube.com/watch?v=ul1eden8ja4
- https://www.youtube.com/watch?v=OW3_BsAtcr4
- https://www.youtube.com/watch?v=W7agCnQqKh4
- https://www.youtube.com/watch?v=Ag2AyHVNSw8

Icons

- Presentation icons downloaded from Flaticon.
  - https://www.flaticon.com/

Thank you!

Was this helpful?

YES

NO