CAREERS EBOOK

Cyber
TALENT PARTNERS

Hack your way into Cyber

The Recruiter’s guide to entering the world of cybersecurity. Discover insider tips, strategies, and industry secrets to kickstart your career journey. Whether you're new to the field or seeking a fresh start, this comprehensive resource equips you for a successful career in cybersecurity.

What's inside?

02

WHY CYBER?

The demand for cybersecurity professionals is rapidly increasing due to the evolving threat landscape and growing reliance on digital infrastructure across various sectors. This high demand ensures job security and numerous career opportunities, especially as cyber threats become more sophisticated. Cybersecurity roles offer competitive salaries with potential for growth, ranging from entry-level salaries of £25k to £35k to experienced professionals earning between £70k and £85k on average. The industry provides continuous learning and growth opportunities in various specialisations, offering meaningful work in protecting digital assets and systems, giving professionals a sense of purpose and fulfilment.

- Variety of Roles & Specialisms
- Job Security
- Meaningful Work
- Increase in Demand
- Continuous Learning & Growth
- Competitive Salaries

WHERE TO START

03

The right time to start your cybersecurity career is when you feel adequately prepared and motivated. It's an industry that values lifelong learning, so don't be discouraged if you're starting later in life; many successful cybersecurity professionals began their careers in other fields and transitioned into cybersecurity. The key is to stay dedicated, keep learning, and gain practical experience along the way.

Self-Assessment

Reflect on your interests, skills, and strengths. What aspects of cybersecurity fascinate you the most? Are you more interested in technical aspects like penetration testing or more focused on education or risk management and compliance?

Research

Explore the different domains and specialisations within cybersecurity. Read articles, watch videos, and follow industry blogs to gain insights into the various roles and their responsibilities.

Talk to Professionals

Reach out to cybersecurity professionals in your network or attend industry events to talk to people who work in different areas of cybersecurity. Their experiences and advice can be valuable in making your decision.

Consider Your Background

Your educational background and/or prior work experience can influence your choice. For example, if you have a strong programming background, you might lean toward roles in cybersecurity that involve secure coding or malware analysis.

Flexibility

Keep in mind that the cybersecurity industry is dynamic, and you can pivot or transition into different areas as you gain experience and knowledge. Your career doesn't have to be set in stone from the beginning. Sometimes, you may need to try different roles to find the one that suits you best. Starting with a broad understanding of cybersecurity and then narrowing down your focus as you gain experience is also a valid approach.

COMMON TECHNICAL JOB ROLES

Starting a career in cybersecurity doesn't solely revolve around penetration testing or working in a Security Operations Center (SOC). While these roles are common entry points and can serve as solid foundations for a cybersecurity career, it's essential to dispel the misconception that cybersecurity roles are exclusively technical.

Understanding fundamental networking and computing concepts is crucial for success in any cybersecurity role, even though the field encompasses a wide range of non-technical aspects as well (as detailed on the next page).

SOC Analyst

Sits within a SOC focusing on monitoring systems for intrusion detection and prevention; will often act as the first line of incident response/escalation.

Penetration Tester

Conducts ethical hacking against an organisation in order to identify weaknesses in network security infrastructure or Web Apps and will often put forward recommendations for improvement.

Security Engineer

Involves configuring and maintaining security tools and technologies (such as firewalls, intrusion detection systems, and antivirus software).

Incident Response

Expert incident handler who will manage the technical response to a security breach. Some input in to intrusion response procedures.

Security Architect

Focus predominantly on High Level Design looking at the workflow and broad controls. Will translate the security policy into technical specification.

Cloud Engineer

Responsible for designing, implementing, and managing cloud-based infrastructure and services for organizations

NON-TECHNICAL JOB ROLES

Policy & Governance

Involved in developing, implementing, and managing an organisation's cybersecurity policies and procedures.

Security Risk Management

Involved in assessing an organisation's risk exposure to cyber threats and develop strategies to manage those risks.

Cybersecurity Compliance

Involved in ensuring that an organisation complies with all relevant laws, regulations, and industry standards for data protection and privacy.

Business Continuity & Disaster Recovery

Responsible for developing and implementing plans to ensure that an organisation can continue to operate in the event of a security breach or other disruptive event.

Security Education & Awareness

Involves developing and delivering training and education programs to raise awareness about cybersecurity issues and best practices.

Security Sales & Marketing

Involved in helping organisations understand the importance of cybersecurity and the benefits of various products and services to protect against cyber threats.

NAVIGATING JOB TITLES IN CYBERSECURITY

06

1) READ JOB DESCRIPTIONS CAREFULLY

Look beyond the title and focus on the responsibilities, skills, and qualifications mentioned in the job description. This will give you a clear idea of what the role actually entails.

2) USE KEYWORDS

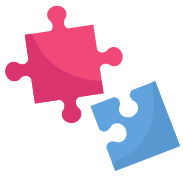
Rather than search for a job title, use a combination of specific keywords related to cybersecurity in your search. For instance, use terms like "network security," GRC or "cloud security" to narrow down your search to roles that align with your expertise.

3) RESEARCH THE COMPANY

Explore the company's website and social media profiles to get a sense of their cybersecurity team's structure and the roles they offer. This can help you decipher the meaning behind unconventional job titles.

4) LINKEDIN & NETWORKING

LinkedIn is a valuable resource. Connect with professionals in the cybersecurity field, and you can learn about their roles directly. Networking events and conferences also provide insights into job titles and responsibilities.

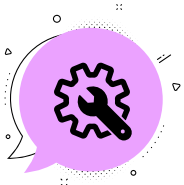


5) REACH OUT TO RECRUITERS

If you're unsure about a job title's responsibilities, reach out to recruiters or Hiring Manager's. They can provide additional context and help you understand the role better.

6) INDUSTRY CERTIFICATIONS

Look at industry-standard certifications like CISSP, ISO27001, and CSTM to understand the skills and knowledge required for different roles. This can give you an idea of the job's focus and/or seniority which will help you to decide if it aligns.



7) CUSTOMISE YOUR APPLICATION

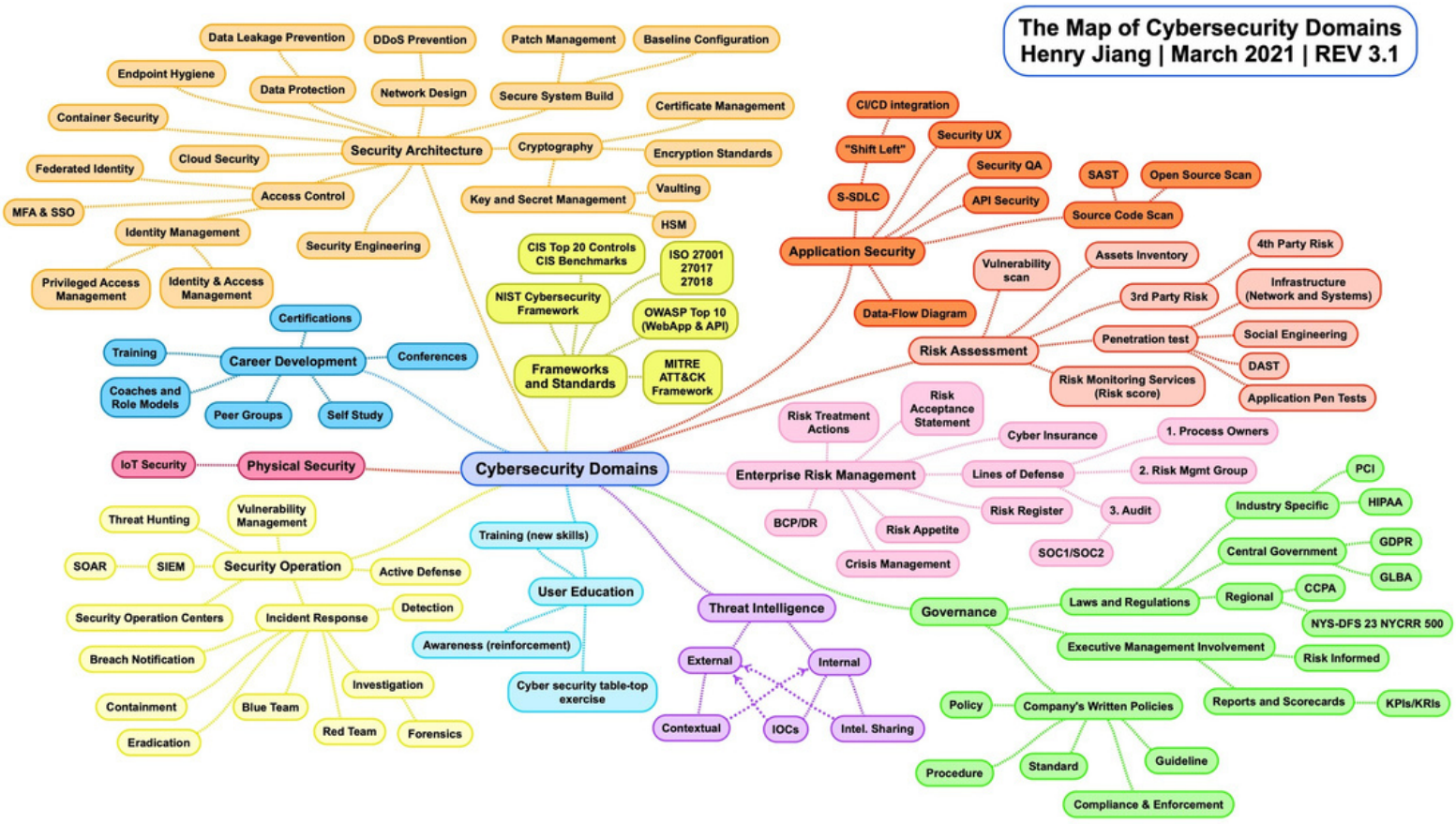
Tailor your CV and cover letter to highlight your skills and any previous or similar experiences that match the job description, regardless of the job title. This will demonstrate to recruiters and employers, why you're a good fit for the role.

CYBERSECURITY DOMAINS

07

As you'll observe below, cybersecurity encompasses a wide range of disciplines. While they may seem separate in the presented heat map, these disciplines are intricately interconnected and collaborate to form a holistic approach to safeguarding computer systems, networks, and data.

For example, consider the relationship between risk management and ethical hacking or penetration testing. Risk management involves the identification and assessment of potential security risks and vulnerabilities within an organisation's systems and processes. Ethical hacking is an integral component of the risk management process, where security professionals simulate real-world attacks to pinpoint vulnerabilities and weaknesses. The outcomes of penetration testing play a crucial role in shaping risk management strategies, offering valuable insights into areas that require mitigation and remediation.



08

LEARNING FUNDAMENTALS

You don't necessarily need a highly technical background for a career in cybersecurity, but it's helpful to have a foundational grasp of the following concepts...

Networking Fundamentals

Understanding how networks operate, including TCP/IP, routing, subnetting, and common network protocols, is essential. Networking knowledge helps you analyze network traffic, identify anomalies, and assess vulnerabilities.

Operating Systems

Familiarise yourself with various operating systems, especially Windows and Linux. Learn how to or the process of how to configure, secure, and troubleshoot these systems.

Cybersecurity Concepts

Develop a strong understanding of core cybersecurity concepts, including threat actors, attack vectors, security controls, cryptography, and security frameworks.

Security Tools

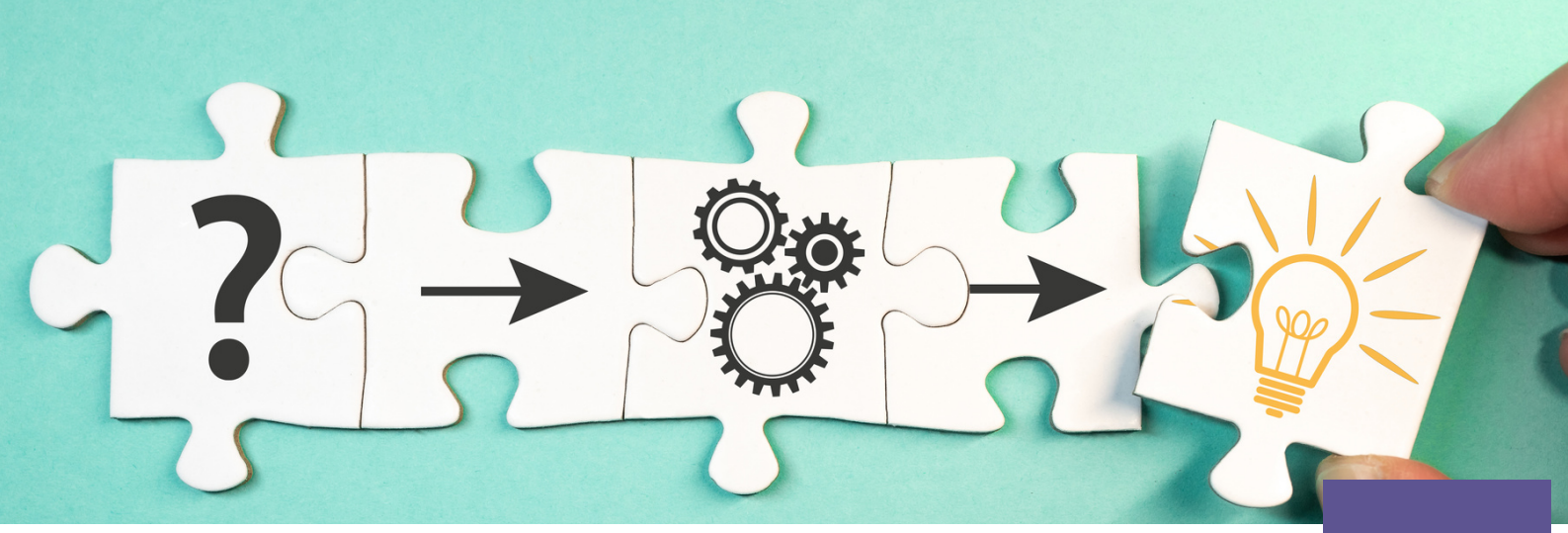
Build knowledge of common cybersecurity tools, such as Wireshark for network analysis, Nmap for network scanning, and Metasploit for penetration testing. Familiarity with security information and event management (SIEM) systems is also valuable.

Firewalls

Learn about firewalls, IDS/IPS systems, and how they work to protect networks and detect suspicious activities.

Cloud Security

Gain knowledge of cloud security principles, as many organizations are migrating to cloud environments. Understand the shared responsibility model and cloud-specific security challenges.



SELF STUDY RESOURCES

09

Self-study is crucial in cybersecurity due to its fast-paced nature and the need for practical experience. It offers flexibility, cost-efficiency, and the ability to personalise your learning, helping you stay updated with evolving threats and technologies. Self-study also demonstrates your initiative and commitment to potential employers, fostering a habit of continuous learning, which is vital in this industry.

General Cybersecurity

FutureLearn - Introduction to Cybersecurity Course
SANS Cyber Aces Online
Cybrary - Introduction to IT and Cybersecurity
Pluralsight Cybersecurity Courses
Fortinet NSE Institute Self-Paced Content
Coursera - Security Analyst Fundamentals
UK Cybersecurity Council

GRC

Pluralsight - The Governance of Information Security
FutureLearn Cyber Threats and Risk Management
Professor Messer's online risk-related content
Security+ online content - Cybrary, Professor Messer
ISO27001 resources - FutureLearn, BSI, ISO27001 Basics, ISO27001 Videos

Network Security

Professor Messer's online content, Cybrary
Network Security Basics - Pluralsight, FutureLearn
Cisco Networking academy
Jeremy's IT Lab CCNA course
Graphical Network Simulator-3
Network Security (Ed X)

Penetration Testing

TryHackMe
HacktheBox
OverTheWire
Udemy
Penetration Testing — Discovering Vulnerabilities [edX course]

**** We will regularly expand and improve this list as we come across additional valuable resources.****

RESOURCES CONT.

Meet Up's

Ladies of London Hacking Society
WiCyS - Women in Cybersecurity UK
Hack Thursday (Glasgow)
TechVets

Conferences

DTX London & Manchester
BSides
International Cyber Expo (ICE)
Infosec Europe
Cloud & Cyber Expo
Cyber UK (Birmingham)

CTF's & Activities

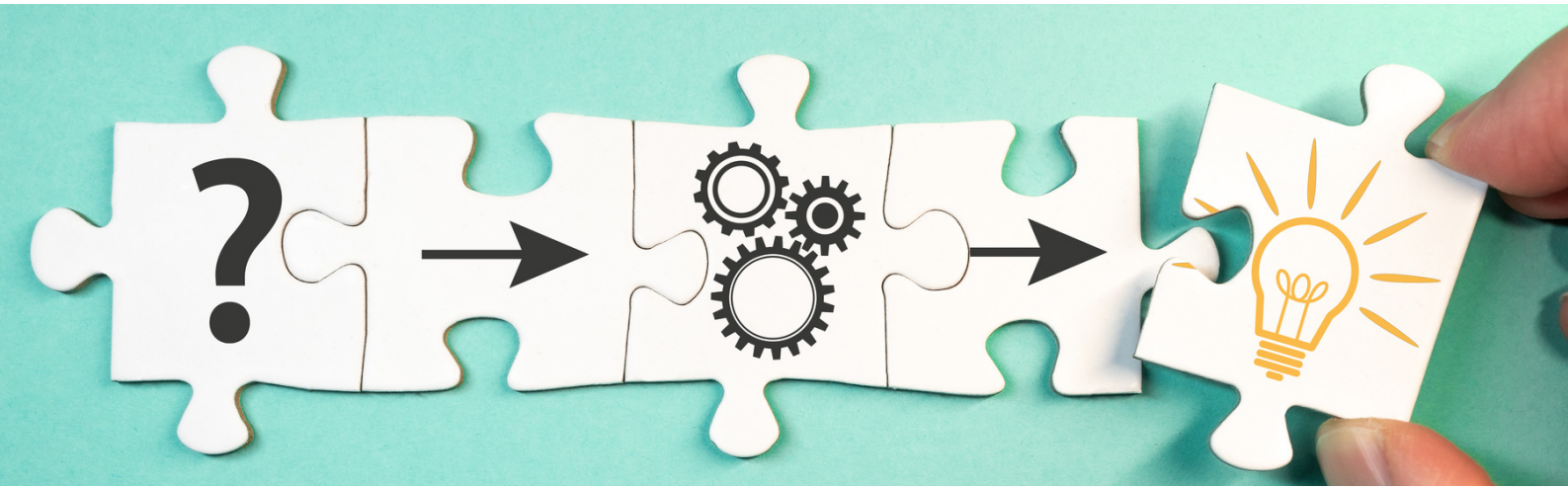
OWASP
Trace Labs - (Disclosure: Exposure to sensitive information).

People to Follow

Mollie Chard - Early Careers
Will Broom - Early Careers
Jay Jay Davey - Blue Teaming/SOC
Lisa Forte - Risk, Crisis Management
Nikki Webb - Godmother of Security
Holly-Grace Williams - Pentesting
Sarah Armstrong-Smith - General Awareness

Talks, Podcasts & Blogs

Darknet Diaries
Basics of Risk Management - Tom Quinn
Flipper Zero - James Bore
Threat Intel Blog - Will Broom
Threat Modelling - Dann Conn
Application Security Testing - Holly-Grace Williams



TIPS TO BUILDING YOUR NETWORK

11

BENEFITS

- Access to Opportunities
- Mentorship & Guidance
- Learning & Skill Development
- Resource Sharing
- Personal Branding

TIPS

- **Online Networking:** Utilise professional networking platforms like LinkedIn to connect with professionals. Join relevant groups and engage in discussions.
- **Attend Events:** Attend industry conferences, webinars, and seminars. These events provide opportunities to meet professionals and learn about the latest trends.
- **Local Meetups:** Look for local professional meetups, workshops, or networking events In-person interactions can be very valuable.
- **Volunteer or Intern:** Where possible, consider volunteering or interning. This hands-on experience allows you to build connections while gaining practical skills.
- **Professional Organisations:** Join industry-specific organisations or associations. These groups often host events and provide access to a network of professionals.
- **Informational Interviews:** Reach out to professionals for informational interviews. This is a great way to learn from experienced individuals and expand your network.
- **Offer Value:** Networking is a two-way street. Offer your skills, knowledge, or assistance to others in your network when possible.
- **Stay Active:** Consistency is key. Regularly engage with your network, share insights, and maintain relationships.
- **Follow Up:** After meeting someone, always follow up with a thank-you email or message. A thoughtful follow-up can strengthen your connection.
- **Networking Plan:** Create a networking plan with specific goals and strategies for building and nurturing your network. For e.g. grow your connections by 20 people per day.

Linkedin ‘How to’ Guide

Your Linkedin profile page is the foundation for your personal branding. This is a great way to demonstrate your skills, motivations and interests, think of it as your digital CV. Even if you are not actively seeking a new job, just having a well-structured profile could change your career!

Other benefits of a Linkedin account mean you can network with like-minded individuals, get involved in forums and join interest groups. Another advantage of having a Linkedin profile is that it can help open doors to opportunities that may never have existed previously but having an incomplete or unprofessional profile can also have a detrimental effect and portray a negative impression to potential contacts and/or employers.

TIPS TO BUILD A WINNING PROFILE

13

#1. Clean URL	Having a more professional, clean, name-only URL is much easier to find, read, and share. • Go to your profile • At the top right of your profile page click “Edit public profile & URL” • Again at the top right of the page now click the edit pen image button • Fill in “[First Name] + [Last Name]”
#2. ‘Professional Headline’ and ‘Summary’.	This is the most important part of your Linkedin profile and is what visitors to your profile see next to your name. This needs to include your career focus and components of your work or professional interests. Having the right headline ensures you get found by recruiters/hiring managers for the right, relevant job, since many of them only search by title or keywords. Eg. Aspiring cybersecurity professional | Curious about GRC
#3. Profile summary	This should provide a deep insight about what makes you unique, where is your career headed, how would others describe you, what are your values and personal traits? -Include industry related keywords, core skills, your strengths/talents and professional interests -It can be read in 30 seconds Try to structure your summary as follows; • Description of what you did in your previous career, not only your job title, think more about the impact and value your work had to the business/client/customer/end user. • If changing career, why? What motivated you to pivot your career? •)What are your top transferable skills or what do others/ex-colleagues think are your top skills? • What is your career goal? Do you want to be recognised as an expert? In what area and why? • Do you have a personal goal, are you passionate about making a difference somewhere or to something? What and why? **Do's** • Make it between 3 and 5 paragraphs long • Use clear, concise sentences • Separate the information in structured paragraphs • Use bullet points when relevant **Dont's** • Make it too short - one sentence won’t do • Make it too long - Your point will get missed! • Copy and paste a generic summary - You want to stand out, not fit in!

CONT.

#4. Work Experience	• Listed in reverse order, current job at the top. • Link job to the company • Clearly state your Job title • Brief overview, use 1 or 2 sentences to give the reader an overview of what your job involved/s, what is your purpose and responsibility? • List achievements/high level role objectives as bullet points approximately 3-5.
#5. Education	Don't forget to add all learning and development, courses, certificates. Anything big or small. This shows your commitment to personal development, even if not for your job. This isn't just for school/college/university. Demonstrating continuous self -directed learning is absolutely critical in this industry, which evolves rapidly. How do you/will you stay ahead of the curve and learn about new developments/tech/industry intelligence?
#6. Skills & Endorsements	• Adding a list of skills on your profile helps other understand your strengths, it also allows other people in your network to endorse you. This will also enable Linkedin to match you with opportunities and recommend new connections. • Ask people in your network, colleagues, clients or associates to endorse your skills that they have experienced (remember you need to be highlighting your transferable skills now). That is the purpose of this section so don't be embarrassed to ask. You could endorse your connections first which will prompt them to return the gesture.
#7. Reccomendations	• These should come from former managers, colleagues, clients, vendors, professors or fellow students. (Basically, anyone who will have good things to say about you and your work.) • Identify a reason for wanting recognition, this isn't just about improving your chances of getting a new job, its about positioning yourself as the professional you want to be known as, and there is nothing more credible and powerful than other people recognising you for your skills and achievements.

CV WRITING GUIDE

15

Your shop window

Stand Out

- Display all relevant skills
- Include portfolios of work to demonstrate ability without commercial exposure
- Community events - Show any participation / volunteer work
- Mention home labs, resources you use and CTFs you have taken part in

Sell Yourself

- Use the STAR method
- Include an Elevator Pitch in your intro
- Get testimonials
- Does it add value? If not, lose it

Do's & Don'ts

- Don't include a personal photo
- Don't feel you need to stick to two pages
- Do write in first person and talk about I instead of we
- Do use spell check and proof read

STAR Methodology

Can be used for interviews, cv writing, blog posts and linkedin

Situation
Explain the situation that you were in. This should be a short description, such as: 'during my Security assessment project at Capslock / SANS / own personal study'

Task
Briefly explain what it is that you did, and what the success criteria was. If you were working as a group explain what the overall task of the group was but be clear about your own role.

Action
This is the most substantial part of any example, you need to include:
What you did
Why you did it
How you did it
What skills you used

Result
Be prepared to explain:
What happened as a result of the actions you took?
What you would do differently or improve?
What impact the result had overall on the team task?

Checklist

- ☑ Have you used an example that is up to date and relevant?
- ☑ Have you spoken/written about action that you took, not just as a whole team?
- ☑ Does the task or action relate to the company's role as much as possible?
- ☑ In the action part of the example, have you covered the skills and qualities that are being sought?
- ☑ Did the example have a positive outcome?
- ☑ Have you been clear and concise?

CV FORMAT & INFORMATION

Contact Details

Make sure to include:

- Your name
- Address to include town and county
- Telephone numbers including mobile
- Email address
- LinkedIN profile

Personal Profile

Summarise any experience and what aspects of security you are interested in.

If you are applying for different roles, tailor this every time to the job. For example, if the spec is asking for a Cyber Analyst with experience of implementing new SIEM solutions and you have volunteered or completed a placement in a similar field, make it known.

If the spec is asking for knowledge of certain technologies (or equivalents), again, make it known on your CV – list these on your CV according to what the job is asking for

Don't be afraid to list your career aspirations. If you want to be a Penetration Tester within a Consultancy so that you can gain more exposure, put this here.

Add any extracurricular activities i.e. CTFs / Blogs / Conferences / Speaking engagements / Volunteer work that is relevant to the roles you are applying for, to showcase your passion.

KEY ACHIEVEMENTS

STAR

Task Example: "I recently volunteered at BSides London and set up the rig for the on-site CTF competition. This meant that we could monitor the activity of the participants in real-time and trust that the winning team was actually deserving of the prize, as well as offering support to those looking to learn and develop whilst they completed the challenge."

- Include achievements that are related to the skills required in the position you are applying for.
- You should include details of a situation you were involved in that resulted in a positive outcome - if you can describe the results you got in a commercial sense it demonstrates a strong business awareness.
- You should describe the tasks involved in that situation, talk about the various actions taken and the results relating to these.
- Employers want to know that you have solved problems similar to theirs and that you achieved results.

EDUCATION & TRAINING

TOP TIP

Include current certifications and training and any aspirations you have, and certifications you are working towards

- List any technical qualifications that are relevant – for a graduate role include your full education history.
- If you are concerned about your lack of qualifications don't worry, many highly regarded business professionals do not have academic or technical qualifications. Good employers generally value experience and aptitude over certs.
- If in your spare time you are completing CTFs and challenges on HTB Vulnhub etc., put this in here. If you are starting out and looking for a new opportunity, it is these types of things that will make you stand out from other applicants, along with your portfolio

CAREER HISTORY

TOP TIP

Don’t be afraid to include work you don’t think is relevant. If you worked in a restaurant at the weekends, it shows that you can work well in a team, can effectively manage your time, manage well under pressure, communicate with a variety of people, sell, and was trusted to handle money, etc. It also shows you’re not afraid of hard work.

Format: Title held, Name of company, Dates of employment (month and year)

- Include any volunteer work, part time and placement work here too! If there are gaps, explain why and add any information such as “part time work during my studies at X College” – this shows a good work ethic
- Start with projects you have enjoyed whilst studying. Think – how would I describe it to my parents? E.g. Security Consultant can mean many things so what makes you unique is the specifics.
- What projects have you worked on? What did you achieve? E.g. pen testing a mobile application on a personal project to ensure the security of personal data.
- What technologies did you use? Did you work to a particular framework?
- What were you trying to achieve and in what timescales? Did you complete it on time? Did you work on multiple projects with conflicting deadlines – put this in.
- Did you have to interact or report to any other functions or departments? Did you lead a team?
- Did you have to work to a budget or manage one?

ANYTHING ELSE

TOP TIP

Add anything extra-curricular that demonstrates passion and valuable skills

Do you listen to Darknet Diaries, have you volunteered for a Trace Labs Search Party?

This is your opportunity to close and leave them impressed with all the extra work you've done – include anything relevant to the industry

- Mention any Professional Memberships. Are you a OWASP Member? If not it's easy to be.There are lots of other networks and associations you can join that are very cheap or free that will give you access to more events, information and advice.
- Have you submitted any CVEs? Include full details.
- If you have created any blogs, led any societies, published any papers, taken part in any speaking engagements, etc. put this information here!
- Have you won any awards or commendations for your work, paid or otherwise? – include it!
- "References available on request" – it's best to protect the details of your referees, do not include their contact information on your CV. Employers don't need this information within the early stages of the recruitment process but do feel free to include testimonials with simply job title, and industry of the person who wrote it.

INTERVIEW TIPS

#1

Research the Company

Understand the company's mission, values, products or services, industry position, recent news, and any specific job details. This knowledge demonstrates your genuine interest.

#2

Review the Job Description

Review the job descrption to identify the key responsibilities, required skills, and qualifications. Tailor your responses to align with these requirements.

#3

Practice Common Interview Questions

Anticipate common interview questions like "Tell me about yourself," "Why do you want this job?" Practice your responses to these questions.

#4

Prepare STAR Stories

Develop specific examples of your achievements using the STAR method (Situation, Task, Action, Result). These stories illustrate your skills and experience.

#5

Prepare Questions

Prepare thoughtful questions to ask the interviewer. These might focus on company culture, team dynamics, or the future of the role.

INTERVIEW TIPS CONT.

20

Landing your dream job goes beyond just acing industry-specific or technical questions. It's about building a meaningful connection with your potential employer.

Why do personal questions matter?

Hiring managers aren't just looking for the perfect skill set; they're seeking the right cultural fit and a genuine passion for the role. Personal questions are their way of diving deeper into who you are as a person and what drives you beyond your professional life.

Here’s some quick tips to prepare for those personal inquiries:

💡Authenticity is your best asset. Share genuine stories and experiences that showcase your personality, values, and character. It's your unique story/stories that can set you apart from other candidates!

💡Find ways to relate your personal interests to the role you're applying for. Perhaps your love for travel shows adaptability, or your passion for community service demonstrates your teamwork and empathy.

💡While personal questions aim to reveal your character, maintain professionalism in your responses. Be mindful of boundaries and remember that you're still in a formal interview setting. But be human!

💡Ask Questions Too: Interviews are a two-way street. Don't hesitate to ask the interviewer about the company's culture and values. This shows your genuine interest in finding the right mutual fit.

So, the next time you prepare for an interview, remember, it's not just about what you know but who you are! Be ready to share your story, your values, and your passions. This holistic approach to interview preparation can make all the difference in finding your perfect fit!

Adam Pilton

Senior Cyber Security Consultant at CyberSmart

What was your previous career before transitioning into cybersecurity?

I was a Police Officer for 15 years.

What motivated or inspired you to make the transition into Cybersecurity?

For the last 6 years of my police career I got involved in digital investigations and investigating cyber crime. I loved the continuous learning and found the digital world so interesting.

Where did you start first and how did you know which area you wanted to go into?

I was fortunate. I joined LinkedIn to see what opportunities there were within cyber. By chance, I saw a post by a recruiter who was looking for candidates for a role within cyber. This Intrigued me, so I reached out. That job wasn't for me, but the recruiter took my details and weeks later contacted me about a role as a cyber security consultant at a start up.....a few months later I had left the Police to join the start up!

What were the biggest challenges or obstacles you encountered during your career transition? How did you overcome these challenges?

I couldn't see how my skill set fitted into to the role. I didn't know ISO27001 inside out and because of that, I doubted myself. However, once I was given a project, I worked hard and made sure that if I didn't know something I learnt it. This led to great results for the project.

What educational resources or courses did you find most valuable in preparing for your cybersecurity career?

YouTube. Watching videos to top up my knowledge or refresh my memory has been a real help. Network Chuck has become a real favourite of mine!

Did you pursue any certifications, and if so, which ones were particularly helpful?

CompTIA Security+ felt like a big one to me at the time. It was the first exam I had taken since leaving the Police and I had studied 100% in my own time, over evenings and weekends. Obtaining that felt like I had a cert that was recognised by the industry. Before that, all of my certifications were Police based and most people had no idea what they were.

Adam Pilton Cont.

What specific technical and non-technical skills did you prioritise developing for your new career?

I was fortunate to be working within digital investigations within the Police. I had received lots of training in the Police on Networking and Cyber hygiene. So I was able to use this to talk the language of my peers and support my clients.

How did you go about acquiring and honing these skills?

I spent lots of time on evenings and weekends studying for exams and this ensured my knowledge was continously growing.

Did you seek out mentors or join professional networks related to cybersecurity?

The only network I started to use and join was the LinkedIn network. Although at the time, I rarely posted anything.

Can you share any advice on building a network in the industry? If so, how did that help you?

I would 100% recommend going to industry events such as InfoSec and Cyber Expo. This is a great opportunity to listen to peers talking and having the chance to chat with your peers too.

Were there specific strategies or resources that helped you secure your first cybersecurity role?

I felt like on both my jobs post Police, I was fortunate to find them. The key to.both though were recruiter's that I had met on LinkedIn.

How has your career evolved since you entered the industry?Have you taken on different roles or responsibilities along the way?

Yes, I started out looking more at cyber security frameworks and heavily focusing on consultancy. I have now changed roles and added a more technical element to my daily life.

What advice would you give to individuals who are considering a career transition into cybersecurity?

Believe in yourself. I have found that particularly within cyber security it is easy to think you don't know the answer or someone else knows better than you. This isn't the case and often the conversation benefits from varied opinions and views. Speak up!

If you want to learn more about Adam or follow his career journey you can do so **here**.

Dan Conn

Senior Platform Security Engineer at Trustpilot.

What was your previous career before transitioning into cybersecurity?

I grew up in humble beginnings, tinkering with programming on an old computer from 1982. My understanding of the cyber world was shaped by the 1995 film "Hackers," unaware that software development could be a viable career.

At 14, I delved into DJing in nightclubs, balancing this passion with sporadic gigs and odd jobs until I settled into a stable, albeit unfulfilling, role as a warranty administrator at a car garage for 8 years. Simultaneously, I dabbled in web development for local bands, realising later that I probably wasn't charging enough!

A friend recognised my potential and invited me to work as a developer, coinciding with my pursuit of a BSc in IT and Computing. Despite the challenges of an unstable educational landscape post-financial crisis, my degree instilled in me sound engineering principles.

My career took a security turn after handling a hacking incident, prompting me to delve into secure coding practices.

Subsequently, my journey led me to Mimecast for five years, immersing me in high-level security practices.

At this time I also studied for an MSc in Cyber Security and Digital Forensics at Edinburgh Napier part-time. I loved this course and learnt a lot. Sadly due to the increased workload of COVID, and personal reasons, I didn't complete my dissertation and accepted a Postgraduate Certificate instead, which I'm hugely proud of.

Presently, at Trustpilot, I've discovered my passion for application security, inadvertently transitioning from software engineering into this fulfilling domain. My diverse interests also encompass penetration testing, cryptography, OSINT, and malware analysis, areas that seamlessly align with my coding background.

Dan Conn Cont.

What were the biggest challenges or obstacles you encountered during your career transition? How did you overcome these challenges?

The pivotal moment for me was in the car garage, thinking I had hit my career peak. Taking the leap to study, whether through bootcamps, university, or self-learning, is daunting. Financial sacrifices and imposter syndrome plagued me initially, but I realised my worth through consistent growth. Balancing study with family demands was tough, yet prioritising self-improvement ultimately benefits everyone.

What educational resources or courses did you find most valuable in preparing for your cybersecurity career?

Firstly, when you study in formal education, you get a lot of lectures and material given to you. But on top of that, the internet is a treasure trove of good information! There are many blogs on a whole range of cyber security subjects.

For application security, look at the awesome materials and tools produced by OWASP. The Linux Foundation provides great courses on network security. Physical Security check out Freakyclown's book “How I Rob Banks” and “People Hacker” from Jenny Radcliffe.

Michael Bazzel's books on OSINT are a must as are online resources from Tracelabs and Bellingcat. If you're still unsure what direction to take two great reads are also “Breaking Into Information Security” by Andy Gill and “Confident Cyber Security” by Jessica Barker.

I possess absolutely no certifications at the moment. But actually, this may change in the future.

I would say if you feel that spending the money will definitely give you something that you value then go for it. Pick ones that provide good general knowledge that don't tie you to specifics too. For, example if you're starting today and you want to get into networking then maybe AWS or GCP certification may make sense as some job descriptions may demand it. But ten years ago it was Cisco CCNP. Also CISSP can be useful, but it's a meant for people with many years practical experience.

What specific technical and non-technical skills did you prioritise developing for your new career?

I think most skills I obtained over time in different areas so I don't think I needed to learn anything new as such.

Dan Conn Cont.

Although I personally think that in both software and cyber, being able to code in different languages and having an appreciation of how data moves through a system and gets processed has been a huge help.

Also the ability to communicate effectively. You may need to speak to different levels through the business in various levels of detail. Writing coherent reports, PowerPoints, charts all help get your message across. Weirdly enough these skills came from DJing, doing an NVQ in Conflict Management and during my office admin days. You'll find skills you already have are hugely transferable!

Did you seek out mentors or join professional networks related to cybersecurity? How did this support your transition?

I did but in an informal setting. Use social media such as LinkedIn, Twitter, Bluesky and others to connect with people in the field. #MentoringMonday is a great way to connect with people who have mentoring time to give.

Go to conferences like BSides and network. I was very fortunate to put myself up for speaking at The Beer Farmers BeerCon which provided some great mentors that I still talk to. Use online Discords too. Everyone is pretty friendly so definitely use it to your advantage, but be mindful of their time.

Mentoring is normally free and isn't something people may have a lot of time for beyond s chat and some pointers. There are paid coaches too, but if you're paying money, make sure the person is respected in their field and can add value.

Were there specific strategies or resources that helped you secure your first cybersecurity role?

Get a LinkedIn profile that is a full honest reflection of your skills and network with recruiters.

Voluntary work for orgs like OpenUK, OWASP, or open source projects are a great way to gain experience, but also think about a problem you want to solve, and create your own project - then think about how to secure it and do that!

Dan Conn Cont.

How has your career evolved since you entered the industry?

Progression is not always linear. I've gone for mid-level developer roles, to senior, back down to mid-level but dealing with much larger scales. I've line managed, been in control of budgets, mentored, given presentations but always been seen an an individual contributor.

I like to look at the next big thing and demistify it. Sometimes it's beneficial, other times I realise it's not for me. Progression isn't always about more money. It's about well-being, improving your skillset, seeing what another company can do for you what can't be fulfilled by the one you're currently at.

What advice would you give to individuals who are considering a career transition into Cybersecurity?

Do it! Get involved in the ways mentioned. Start with general knowledge, even subjects that you find boring. Test how it sits and then go deeper into the things that interest you. Seize the day and see what works for you.

If you want to learn more about Dan or follow his career journey you can do so **here**.

Dawn O'Connor
Co-Founder
Shift Key Cyber

What was your previous career before transitioning into cybersecurity?

My background has been a varied one. I have a background in psychology and have had other roles such as working in retail management and risk and compliance.

What motivated or inspired you to make the transition into cybersecurity?

Risk and compliance have always played a part in many of my roles. I knew a few people who worked in the cyber security industry and from talking with them I knew it was the right career step.

I really like the fact nothing stays the same; threats are ever evolving, and we need to be continually learning and improving as professionals to help customers stay secure - that is the biggest motivator for me.

Where did you start first and how did you know which area you wanted to go into?

After leaving my management role I took some contract work whilst I self-studied and achieved a couple of certifications.

This gave me the confidence to apply for a cyber security consultancy role where I was successful. It was for a large organisation, which became clear over time was not for me. Although grateful for the experience I wanted a job that aligned with my values, and I wanted to work in a smaller consultancy environment. So, I made the decision to leave, and I started volunteering in industry. I was very fortunate to have an existing contact who gave me the opportunity to co-chair the East Midlands branch of the Chartered Institute of Information Security. This allowed me to get involved in a few projects and I was able to continue to self-study.

I knew with having a background in psychology, risk, and compliance I would thrive in a governance, risk and compliance (GRC) role. I love the variety, and it really aligns with who I am and my skill set.

Dawn O'Connor Cont.

What were the biggest challenges or obstacles you encountered during your career transition?

The biggest obstacle for me was me, and the belief in my own ability and my place in the industry.

How did you overcome these challenges?

I believe success is an inside job and you have to meet yourself where you are. We become so focused on the end goal that we don't appreciate the journey we are on, or more importantly celebrate the small wins. Our fear of rejection often creates a blocker to our success so even if you do not get the job or pass an exam you have shown up for yourself and taken a risk, celebrate that. We should never underestimate how much personal growth there is in those moments, even if it does not feel it at the time.

I began trusting my decisions and learning from the outcomes because the alternative was to stay stuck and not move forward in a career I wanted. I surrounded myself with people who shared the same values that I did, who were already working in the industry who kindly gave me their time and experiences and I started to say yes to more situations and events that I would normally shy away from. I felt in safe hands with my network who were both encouraging and great at providing feedback, and this shift opened up my network further and created more learning opportunities.

What educational resources or courses did you find most valuable in preparing for your cybersecurity career?

After working in industry for a short time and engaging in personal study I decided to do the CAPSLOCK course. I wanted a more structured approach to my learning, and I wanted to baseline my knowledge to that point.

Did you pursue any certifications, and if so, which ones were particularly helpful?

I completed CISMP and ISO 27001 Foundation a few years ago through self-study. Both are good for providing foundational knowledge. I think Comp TIA Sec + is also great exam to get started for the more technical elements. In my role, I work on projects utilising the ISO standards (ISO 27001 and ISO 22301) and have obtained further certifications in those. Whenever I choose to take a certification, it must be relevant to my role so that I can apply it otherwise it is just another certification and a waste of time and money.

Are there any resources you found particularly useful in helping you towards the area you work in now?

One of the many resources I refer to is the National Cyber Security Centre website; One thing I will say, it is vital to find trusted sources for information and this one is hands down one of the most valuable in my role.

Dawn O'Connor Cont.

What specific technical and non-technical skills did you prioritise developing for your new career?

From a technical perspective having a fundamental understanding of network architecture is key, although my role is classed as non-technical, I prioritised getting up to speed with these aspects.

How did you go about acquiring and honing these skills?

I have studied network architecture and continue to revisit it as part of my ongoing learning plan.

Did you seek out mentors or join professional networks related to cybersecurity? How did this support your transition?

I had a great mentor and I still value her input and honesty today. She is someone I would trust to give me a balanced and objective viewpoint on anything I am extremely grateful and thankful she has played a part in my journey.

I would recommend finding a mentor but again it must be someone that aligns with your goals and values.

I am a member of the Chartered Institute of Information Security and the British Computer Society; both have some great resources and events.

Can you share any advice on building a network in the industry? If so, how did that help you?

Networking for me is so much more than connection requests or going to events, it is about forming relationships based on mutual respect and support. Your network should complement your journey and reflect where you aspire to be. I would say seek out people who align with your values first and foremost and be selective who you surround yourself with.

This has played a huge role in the opportunities I have got involved in and given me many opportunities to be part of a great inclusive community which in turn has contributed to my own development and giving back to the community.

Were there specific strategies or resources that helped you secure your first cybersecurity role?

I think my CV was the most important aspect of my career search, having an honest well laid out CV is key that showcases your strengths and achievements but also your willingness to learn. Volunteering and getting involved in industry events helped me meet people I would never have had the opportunity to meet in day-to-day life, and it also puts you at the forefront of their mind when they are recruiting.

Dawn O'Connor Cont.

How has your career evolved since you entered the industry?

I am now a Co-founder of a female led cyber security consultancy.

Have you taken on different roles or responsibilities along the way?

My role as a co-founder means I wear many hats within the business but as far as my cyber security journey is concerned, I have led and worked on some fantastic projects and have learnt so much along the way. When I first started out, I recognised I was junior in my role regardless of my extensive business background and I needed to learn information and cyber security and apply that learning to develop my knowledge. That journey will be continuous, but I now am more established and work on some great projects. The other co-founder has over 30 years of experience in industry, so I am extremely fortunate to learn from her every day.

What advice would you give to individuals who are considering a career transition into cybersecurity?

I would say do it, it is an extremely rewarding career but be prepared to work and be in a cycle of continuous learning and development. Most importantly be honest with yourself and those around you about what you know and if you do not know something say so. Honesty and integrity will take you much further than saying you can do something you can't.

Are there any resources or strategies you found particularly helpful that you'd recommend?

I ensure every week I put aside time for my own personal and professional development.

If you want to learn more about Dawn or follow her career journey you can do so **here**.

Craig Evans

Threat Detection & Response Manager
norm. Cyber

What was your previous career before transitioning into cybersecurity?

Very limited educational, left college post a Leisure and Tourism GNVQ and went straight into work in Hospitality where I worked for a popular pub chain for 10 years, starting as a shift manager finishing as a General Manager for some Flagship sites in London, I then moved into Retail for a well known doughnut chain for 10 years, working as a Retail Manager, then a General Manager (responsible for Retail, Manufacturing, Warehousing and Distribution) and my last Role was heading up the Store Opening Programme for the UK and Ireland. I then decided on a career change and studied CompTIA A+, Network+, Security+ and EC Council's Certified Ethical Hacker. I then started with norm in October 2020 as an L1 Analyst.

What motivated or inspired you to make the transition into cybersecurity?

Lack of personal satisfaction in my role and career and the birth of my son meant I didn't want to be spending months away from home at a time.

I wanted to make a lifelong change that would allow me to have a continual learning and development opportunity as well as a better life balance.

Where did you start first and how did you know which area you wanted to go into?

I did some research around options that would fulfill the above. I initially thought maybe Human Resources as I had lots of experience and training in that field and had held advisory roles to peers, but I quickly decided that wasn't for me. I started looking into IT as a field just because of its growth as an industry and further investigations highlighted Cyber Security which excited and scared me at the same time. So, I then had some conversations with some training companies.

What were the biggest challenges or obstacles you encountered during your career transition?

The biggest challenge was getting conversations with potential employers, I applied for about 80-90 roles via job boards and couldn't even get a conversation.

Craig Evans Cont.

I realised why would an employer speak to me when they already had CVs for countless Analysts who already were in the industry and knew how to do the job. It was up to me to make that conversation happen.

How did you overcome those challenges?

I moved from Job Boards because it wasn't working, I started to learn how to network leveraging LinkedIn. I had a profile but had never really used it. I started to think about ways that I could demonstrate I was ready to work in the industry whilst growing my network to maximise how many people I was able to reach with my evidence. I would post about methods of protection aimed at those in my network who were not already cyber educated , I would comment on others posts and articles expressing and opinion, talk about my training progress and what I was achieving, Post about projects that I had that showed hands on experience – pen testing labs environments, SIEM lab environments I had built etc.

I also reached out to a lot of industry professionals seeking advice on approaches, what I need to learn, who I should be speaking to as well as making them aware of my progress. The aim for this was to 1) get as much insight as I could and 2) Plant seeds for any vacancies they may have in their organisation.

I also researched companies I thought may have Cyber Security elements in their organisation and then started cold calling in effect to try and get hiring managers on the phone to talk to me.

What educational resources or courses did you find most valuable in preparing for your cybersecurity career?

It's easy to focus on certifications but most of this is theory based with very little practical elements at the beginning and as a result are not as respected as thought they were when I trained. The Theory is important but compliment it with Labs and your own projects. Lots of people talk about labs (TryHackMe,Hack The Box etc) and they are mentioned in every interview I hold. They are great but the things that will help you stand out are demonstrable projects like building your own SIEM and integrating logs, Penetration testing of a network (most likely self-built) and report writing, there is a steep learning curve with some of this but if you can tackle it you will be well on your way to being able to demonstrate why you should be given an opportunity.

Did you pursue any certifications, and if so, which ones were particularly helpful?

I purchased a training pack in order to learn – CompTIA A+, Network+, Security+ and EC CEH. Once I did those I also did Security Blue Team Level 1 which is one of the best entry level courses out there as it relies on practical skills to pass the exam.

Craig Evans Cont.

Are there any resources you found particularly useful in helping you towards the area you work in now?

There is soooooo much content out there its hard to identify what's important to you. Microsoft is a huge part of the world of IT and Cyber so working through their products and gaining an understanding is useful. For Blue Teamers Blue Team Labs online is excellent and will offer you the right level of challenge. Security Blue Team Junior Badge and Level one is great. Identifying your path before applying for roles really helps because it narrows down you field of vision and helps you build a path but of course not everyone is able to do that. I would recommend spending time researching and trying your hand at various areas of Cyber to help. TCM security has some great video led content as well.

What specific technical and non-technical skills did you prioritise developing for your new career?

I was very lucky (although I didn't realise it at the time) that I had 20+ years of experience prior to the transition. I thought I was starting all over again and underestimated the skills and experience I was bringing with me. I don't think I had a narrow enough training plan for myself when I started looking for roles, and if I could do it again I would of looked at Job Descriptions a little closer and used that to map out my training to try and hit as many of those skill sets as possible.

Key demonstratable skills from a soft skill perspective are drive, owning your journey (knowing what you want from your first role, what kind of company you want to work for, what your longer-term aims are) is usually rare and impressive when you come across it. Real commitment to learning and the confidence to fail as some others. We learn more through converting failure to success, for example it doesn't matter if it took you a month to get a SIEM built, and logs ingested. The learning journey associated with that is basically hands on industry experience and shows resilience and determination.

How did you go about acquiring and honing these skills?

Mostly by throwing myself into challenges and working outside of my comfort zone. Don't fear what you can't do today as there is no reason you can't do it tomorrow if your prepared to put the work in. Its not always easy but work the effort.

Did you seek out mentors or join professional networks related to cybersecurity? How did this support your transition?

Absolutely, I would say I had two mentors that I regularly touched in with. One was very technically minded and the other was a leader at Amazon who aided and supported me from an approach and how I portrayed myself perspective. It was invaluable.

Craig Evans Cont.

I had lots of people who offered advice as well some of which I still network with today.

I joined a few Cyber Security groups as well and that typically helped with keeping on top of what was going on in the industry as there were daily post and article sharing.

Can you share any advice on building a network in the industry? If so, how did that help you?

Understand that not everyone is going to want to network, but that's OK. There are still lots of people who will be happy to engage with you (me included) its just finding them and not taking it personally when people do not respond. Start to think of yourself as a Cyber Professional even if you are not already (whilst remaining humble of course) and engaged in comments and article sharing. It's the same as anything in life you reap what you sow so be resilient and get yourself out there.

Consider being a little creative if you post you own content as well. My announcement when I posted I had landed my first role was a picture of me with a keyboard aimed at mimicking a football transfer deadline announcement and I had 30k views. It took me about 5 minutes to create the image.

Networking is also a 2-way street, engage in conversation where you can. You wouldn't just walk up to someone in the street say hi and stand there saying nothing, so when you ask for a connection on LinkedIn don't just send the request, send a message with it, try, and engage them with a message about you and maybe some questions for them to try and get a response.

Were there specific strategies or resources that helped you secure your first cybersecurity role?

Networking, Networking, Networking. From my experience Job Boards and sites have a very low success rate, use networking to complement this. A couple of ways this is useful are 1) increasing your catchment opportunity by increasing your network. The more people who see and can interact with you the better your changes are. 2) Use job boards by all means but where the hiring manager or recruiter is displayed in the advertisement send them a network connection on LinkedIn along with a message. Most don't do this so it will help you engage with the recruiter, likely get them to go straight to your CV to check it and help to put you at the top of the pile. It's a good way of complimenting your application.

Craig Evans Cont.

Tackle ownership of conversations yourself by doing some research and phoning companies you think you would like to work for, again very few people do this, and it may help you get that first conversation. Again, be resilient and thick skinned, not everyone is going to be receptive to this approach but it is another seed to plant.

How has your career evolved since you entered the industry?

I was very lucky that I got to join an organisation who were very open to those looking to enter the industry as well as having rapid growth. This alongside my experience (even thought it was in another industry) led to plenty of opportunity. I moved from an L1 analyst to L2 within 9 months and then to the Manager within 14 months from starting. Since then, we have grown the team substantially.

What advice would you give to individuals who are considering a career transition into cybersecurity?

It's an incredible industry to work in but it won't just happen because you have certifications. I see people think this a lot. There are challenges you will have to overcome but remain determined and resilient and give yourself the best chance by owning your own training and development path and align this to your preferred roles.

Understand that there are lots of people looking to enter Cyber Security, ask yourself the question how are you going to stand out as well as competing for roles with people already within the industry. Develop links and relationships with supportive recruiters as well. Any who take the time to offer you help and advice are an absolute godsend as well. This could be as part of a job application or just via networking, they know the industry and what employers are looking for and likely have a network of organisations they work with consistently as well. If there is not anything suitable today, there may be in future. Having these supportive resources be able to articulate your strengths to potential employers As well of yourself is really helpful.

Are there any resources or strategies you found particularly helpful that you'd recommend?

Sorry to say it again but networking or an element of it is most likely to get you success. Plant as many seeds as you can, it may not bare fruit straight away but may do further down the road. Commit and follow through, it gets results. Also set yourself small targets for example 20 new LinkedIn connections per week and/or 100 views on a post. As you achieve these move the number up and make it a challenge or game, it becomes more enjoyable and helps you identify what works for you and what doesn't to help you continuously improve.

Craig Evans Cont.

Job Descriptions are helpful when you're starting out as it allows you to understand what employers want from you if you're not already in roles, aim to tick 7/10 boxes for example. Hands on training is imperative as it is a technical industry which means a lot of doing and thinking and there is ample paid and non-paid content out there. Personally, I really like what Blue Team Labs Online and Security Blue Team are doing but there are plenty of resources.

If you want to learn more about Craig or follow his career journey you can do so **here**.

CONTRIBUTORS

Natasha Harley - Cyber Talent Partners

Rosie Anderson - th4ts3cur1ty.company

Mollie Chard - Capgemini

Dan Conn - Trustpilot

Tom Quinn - Capgemini