

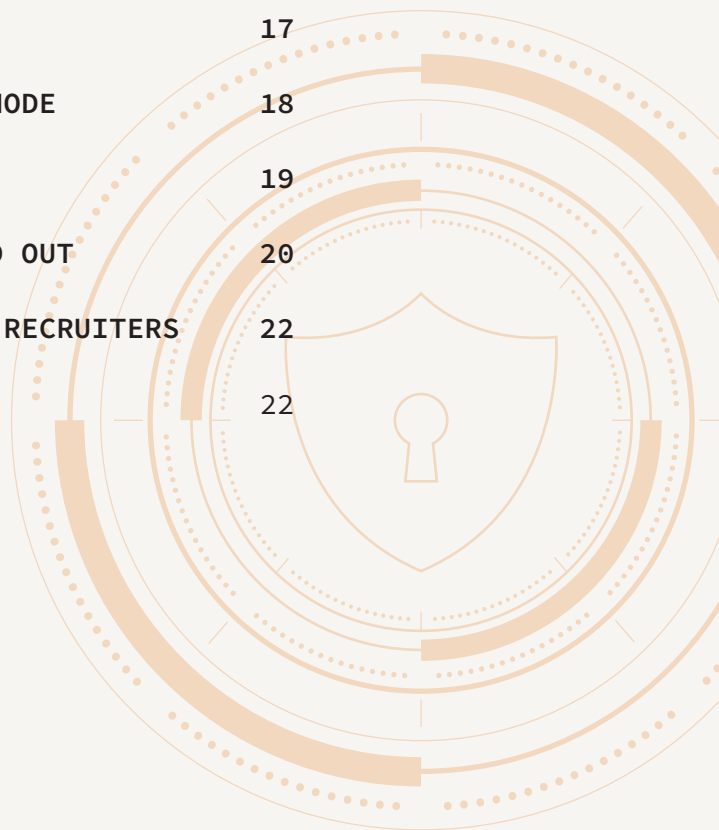
BREAKING INTO THE CYBER SECURITY INDUSTRY

EVERYTHING YOU NEED TO KNOW TO GET STARTED



CONTENTS

INTRODUCTION	3
KICKING OFF YOUR CYBER SECURITY CAREER	4
CYBER SECURITY DOMAINS EXPLAINED	6
CRACK THE CODE TO A CYBER CAREER	10
EDUCATION & CERTIFICATION PATHWAYS: STAY RELEVANT BY STAYING CURIOUS	11
HOMELABS – SHOWCASE YOUR INTEREST IN THE TECH	13
FRAMEWORKS – WHAT ARE THEY AND WHERE TO FIND THEM	14
ROLE TYPES DECODED	15
CODE SHIFT – MAKING A CYBER CAREER CHANGE	17
JOIN THE CYBER COMMUNITY: BE AN ACTIVE NODE	18
NEURODIVERSITY IN THE DIGITAL CORTEX	19
UNLOCK YOUR DIGITAL DISTINCTION TO STAND OUT	20
UNVEILING THE POWER OF CYBER SPECIALIST RECRUITERS	22
CONTACT US	22



INTRODUCTION

.....

This document was collated for the purpose of supporting cyber security careers. Whether you're embarking on your first career or transitioning from another field into cyber security, we hope you find the information included insightful and valuable to carving out a fulfilling career in this dynamic (and we think!) pretty cool industry.

The information and statistics have been collected from Australian professionals at varying stages in their own cyber security journey, combined with our knowledge and experience in supporting and elevating cyber careers for almost a decade.

We reference our Entry Level Cyber Survey, conducted in December 2023 which included feedback from participants with less than one year's experience, right through to participants with 20+ years' experience, and also leaders from some of the largest cyber business in the Asia-Pacific region. In addition to this, we conducted a Round Table Workshop in December 2023, during which participants provided in-depth insights into both their journey through their careers, and what they look for when hiring people into their organisations. This group represented a variety of experience, gender, skills, neurodiversity and roles, which, gave us an excellent snapshot of the views of the cyber workforce as a whole.

We are extremely grateful to the cyber community for their time and contributions, which have led to the insights and advice outlined in this document. It is a true testament to how inclusive and supportive the cyber security community really is.

Enjoy the read,

Jacob Bywater & the e2 Cyber Team



[BACK TO CONTENTS PAGE >](#)

KICKING OFF YOUR CYBER SECURITY CAREER

Embarking on a career in the Australian cyber security industry holds the promise of a fulfilling professional journey, given the escalating significance of cyber security in our contemporary digital landscape.

In the Australian FY22-23 federal budget, the government announced a \$9.9 billion investment over 10 years into our national intelligence and cyber capabilities, creating significant opportunities in the industry. A dynamic, fast-paced, ever-evolving technological environment, it aligns professionals with a “common enemy”. The persistent and evolving cyber threats in the digital realm mean staying ahead is crucial.

“

You have to live and breathe it.

(Senior Architect – Product Vendor)

One of the notable aspects of entering the cyber security domain is the flexibility it offers to newcomers. Unlike other professions, you don’t have to commit to a specific specialisation from the outset. The breadth of the field allows exploration of various certifications, providing a wide array of options. As you embark on this journey, the opportunity to continually broaden your skill set remains a constant, allowing for a more diverse and adaptable learning path.

“

Don’t be afraid of what you don’t know.

(Cyber Partner – Leading Consulting Firm)

Passion plays a pivotal role in this industry, and expressing enthusiasm for the work you’ll be undertaking is crucial. This sentiment is echoed by industry experts who emphasise the need to live and breathe cyber security, embracing the challenges it presents.

Survey results indicate that starting as a Security Operations Centre (SOC) Analyst is a common entry point, with 41% of respondents identifying it as the easiest role in which to initiate a cyber career.

A background in IT helpdesk or tech support is also considered a valuable pathway into the field. The consensus from the survey is clear: be prepared to study diligently and find ways to differentiate yourself in this competitive landscape.

From our experience, the highly competitive nature of entry level cyber roles means the chances of securing a role are quite low. As an example, a pure entry level role e2 Cyber worked on in late 2023 had over 600 applications from one job advertisement alone! Our advice is to look far and wide by applying for service desk, desktop support, ICT support and roles of this nature, as they are an ideal starting point and tend to be easier to secure and start your career.

A solid foundation is essential for success in cyber security. Starting with a strong technical platform and building fundamental skills is essential, with experts advising a focus on understanding and implementing layered security. It’s crucial to recognise that there is no silver bullet solution, and continuous learning and adaptation are key components of success.

[BACK TO CONTENTS PAGE >](#)

KICKING OFF YOUR CYBER SECURITY CAREER

“

Be prepared to study and find ways to differentiate yourself.

(Survey Participant)

Understanding the major fields within cyber security, such as Governance, Risk, and Compliance (GRC), as well as the various specific roles in Red and Blue teams, is essential. Tailoring your path to align with your strengths is advised – whether that's exploring technical aspects or diving into documentation and policy with a GRC focus.

The importance of practical, hands-on experience is highlighted by industry professionals. Learning and meeting supportive colleagues and mentors, contributes significantly to professional development. Recognising that even non-technical roles require a foundation in technology, and a genuine interest in its workings, is crucial for success.

“

Get hands on, learn, meet supportive colleagues and mentors, you'll develop as you learn.

(Survey Participant)

Entering the cyber security profession in Australia offers a wealth of opportunities for those willing to embrace the challenges and continuous learning inherent in this dynamic field. With a foundation of passion, adaptability, and a commitment to ongoing education, aspiring professionals can navigate the diverse pathways available, carving out a rewarding and impactful career in the cyber security landscape.

“

Don't be afraid of what you don't (yet) know.

(Cyber Partner - Leading Consultancy)



[BACK TO CONTENTS PAGE >](#)

CYBER SECURITY DOMAINS EXPLAINED

To give you a comprehensive overview of the industry, we've broken cyber security into 7 core domains, outlining the diversity of both job titles and role opportunities:



ENTRY LEVEL CYBER SECURITY

Entry level roles are diverse but crucial to safeguarding digital landscapes.

Roles include:

- Security Operations Centre (SOC) Analyst
- Junior Cyber Security Governance, Risk Management, and Compliance (GRC) Analyst
- Penetration Testing

Security Operations Centre (SOC) Analysts actively monitor, detect, and respond to cyber incidents, ensuring the resilience of organisational defences. Junior GRC Analysts focus on fortifying cyber policies, assessing risks, and ensuring regulatory compliance to shield against potential threats. Penetration Testing involves ethical hacking, where individuals simulate cyber attacks to identify vulnerabilities in

systems, networks, and applications, offering valuable insights for organisations to fortify their security posture. These roles collectively form the foundation for budding cyber security specialists, contributing to the dynamic and ever-evolving field of digital defence.

“

A SOC Analyst role theoretically provides an entry level candidate to be “in the game” and learning by doing. It allows a candidate to live in the trenches in a way that you cannot do as an outsider.

(Survey Participant)



CYBER ENGINEERING

Cyber engineering encompasses a dynamic and multifaceted field focused on fortifying digital landscapes against evolving threats.

Roles include:

- Junior Security Engineer
- Security Engineer
- Senior Security Engineer
- SIEM Engineer
- Application Security Engineer

Junior Security Engineers play a crucial role in learning and implementing foundational security measures. As they advance, Security Engineers take on more complex responsibilities, designing and implementing comprehensive security protocols.

Senior Security Engineers, with extensive experience, provide leadership in developing and executing strategic security initiatives. SIEM Engineers specialise in Security Information and Event Management, utilising advanced tools to monitor and respond to security incidents. Application Security Engineers focus on securing software and applications, ensuring they remain resilient to vulnerabilities. Together, these roles form a cohesive network of professionals working collaboratively to safeguard digital environments from cyber threats.

[BACK TO CONTENTS PAGE >](#)

CYBER SECURITY DOMAINS EXPLAINED



CYBER ARCHITECTS

Cyber Architects play a critical role in safeguarding digital landscapes against evolving threats, ensuring the confidentiality, integrity, and availability of information.

Roles include:

- Junior Security Architect
- Security Architect
- Senior Security Architect
- Cloud Security Architect

Junior Security Architects are responsible for understanding security protocols and implementing basic measures. As they progress in their careers, they may become Security Architects, tasked with designing and implementing comprehensive security

solutions tailored to organisational needs. Senior Security Architects with extensive experience, lead the strategic development of security frameworks and guide teams in threat mitigation. Cloud Security Architects specialise in securing cloud-based environments, addressing the unique challenges presented by distributed systems. Their expertise in designing and implementing robust security measures ensures the protection of sensitive data within cloud infrastructures, reflecting the ever-growing importance of cloud technologies in today's interconnected world. Collectively, these Cyber Architects form the front line of defence against cyber threats, fortifying digital landscapes in an era where security is paramount.



GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE (GRC)

Governance, Risk Management, and Compliance (GRC) are integral components of organisational strategy that aim to ensure sustainable business practices.

Roles include:

- GRC Analyst (all levels)
- GRC Consultant (all levels)
- IRAP - Infosec Registered Assessor Program

GRC Analysts, at various levels, play a crucial role in evaluating and enhancing the effectiveness of an organisation's governance structure. They analyse policies, processes, and controls to ensure alignment with regulatory requirements and industry standards.

GRC Consultants, also spanning different levels, provide strategic guidance to businesses on implementing robust risk management and compliance frameworks. They collaborate with stakeholders to identify potential risks, develop mitigation strategies, and design compliance programs. Together, GRC Analysts and Consultants contribute to fostering a culture of accountability, transparency, and ethical

conduct within organisations, safeguarding against potential threats and ensuring adherence to regulatory mandates.

Infosec Registered Assessor Program (IRAP), an initiative by the Australian Signals Directorate (ASD), was designed to ensure that cloud services and ICT systems used by the Australian government meet specific security standards and comply with relevant regulations. IRAP endorsed professionals provide advice on security assessments for technical projects, systems and networks and tend to be highly certified, experienced and knowledgeable professionals within both the GRC space and general technology.



www.cyber.gov.au/irap

“

GRC underpins the cyber security culture and posture of an enterprise. You can have the best cyber security technology but if your people are not onboard or do not see the importance of practising good cyber security hygiene, your organisation is vulnerable.

(Survey Participant)

CYBER SECURITY DOMAINS EXPLAINED



CYBER NETWORK

The cyber network is a complex infrastructure that connects computers and devices to facilitate communication and resource sharing.

Roles include:

- Network Administrator
- Firewall Engineer
- Network Engineer
- Senior Network Engineer
- Network Architect
- Network Manager

In the realm of cyber networks, various professionals play crucial roles in ensuring their efficiency, security, and optimal functioning. Network Administrators are responsible for day-to-day operations,

managing user accounts, and troubleshooting issues. Network Engineers design, implement, and maintain the network infrastructure, focusing on hardware and software components. Senior Network Engineers take on more advanced responsibilities, dealing with complex network issues and overseeing junior engineers. Network Architects plan and design the overall network structure, ensuring scalability and alignment with organisational goals. Network Managers oversee the entire network team, coordinating efforts, setting strategies, and ensuring the network aligns with business objectives. These roles collectively contribute to the seamless functioning and security of cyber networks in our increasingly interconnected digital world.



OFFENSIVE SECURITY

Offensive Security encompasses a multifaceted approach to cyber security, employing experts with specialised roles that include:

- Penetration (Pen) Tester
- Red Teamer
- Offensive Security Consultants

Penetration Testers play a crucial role in simulating cyberattacks to identify vulnerabilities within a system or network, providing organisations with insights to fortify their defences. Red Teamers take a more comprehensive approach by emulating real-world adversaries, challenging the overall security posture through advanced tactics, techniques, and procedures. These professionals employ creative thinking to emulate genuine threat actors, offering a holistic evaluation of an organisation's resilience. Offensive Security Consultants leverage their expertise to advise and assist organisations in enhancing their security strategies. Together, these roles contribute to the proactive and dynamic nature of offensive security, ensuring organisations are well-prepared to thwart evolving cyber threats.

Pen Testing

There is always high interest in Pen Testing, but how do you break into that space?

Starting a career in penetration testing, also known as ethical hacking, involves a combination of education, skills development, and practical experience. The key to success in penetration testing is combining theoretical knowledge through education and practical experience through homelabs and work experience. Employers often value hands-on skills and the ability to think creatively and strategically when identifying and exploiting vulnerabilities.



[BACK TO CONTENTS PAGE >](#)

CYBER SECURITY DOMAINS EXPLAINED



CYBER LEADERSHIP

Cyber leadership plays a crucial role in safeguarding organisations against the evolving landscape of cyber threats and guiding the careers of cyber teams.

Roles include:

- Security Officer
- Information Technology Security Advisor (ITSA)
- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)

The Security Officer serves as a frontline defender, implementing and overseeing security measures to protect sensitive information. An Information Technology Security Advisor (ITSA) offers expert guidance, leveraging in-depth knowledge of IT security to advise on best practices and emerging threats. At the executive level, the Chief Information Security Officer (CISO) takes charge of the organisation's overall security strategy, aligning it with business goals. The CISO collaborates with leadership to ensure a comprehensive and resilient cyber security posture.

The Chief Security Officer (CSO) holds a broader role, encompassing physical security and risk management in addition to cyber security. Together, these cyber leaders form a cohesive team, steering organisations through the complexities of the digital age while maintaining the integrity and confidentiality of valuable assets.



[BACK TO CONTENTS PAGE >](#)

CRACK THE CODE TO A CYBER CAREER

There are many paths you can take to kick-start your role in cyber security. At our Roundtable Workshop, it was agreed that starting in an IT helpdesk role can provide a solid foundation for transitioning into a cyber career. There are several ways in which working in an IT helpdesk role can benefit someone aspiring to move into cyber security. It is important to note that the skills listed can also be developed in other roles and applied to a budding cyber career:

Technical Skills Development:

Troubleshooting: Helpdesk roles often involve diagnosing and resolving various technical issues. This helps in developing strong problem-solving and troubleshooting skills, which are crucial in cyber security.

System Knowledge: Working on the helpdesk exposes you to a variety of systems, networks, and software. Understanding how different components interact is valuable when dealing with cyber security issues.

Understanding User Perspectives:

User Awareness: Dealing with end-users regularly provides insight into common security issues and user behaviours. This understanding is essential when implementing security measures that won't overly inconvenience users.

Network Fundamentals:

Network Troubleshooting: Helpdesk roles often involve resolving network-related problems. This experience can enhance your understanding of network protocols, configurations, and security measures.

Firewall and Router Configuration: Exposure to configuring and maintaining firewalls and routers can be a stepping stone toward understanding network security.

Security Incident Response:

Incident Handling: Helpdesk professionals often deal with security incidents, albeit on a basic level. This experience is beneficial in understanding the initial steps involved in responding to security incidents.

Communication and Soft Skills:

Effective Communication: Helpdesk roles require effective communication with users to understand and resolve issues. Strong communication skills are equally important in cyber roles, especially when conveying security policies and measures to non-technical stakeholders.

Certifications and Training Opportunities:

Industry Certifications: While working in a helpdesk role, you can pursue relevant certifications such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH) to demonstrate your commitment to cyber security.

Career Progression within the Organisation:

Internal Opportunities: Many organisations prefer to promote internally. Starting in a helpdesk role can provide you with the chance to move into more specialised roles like system administration or network security within the same organisation.

Continuous Learning:

Learning Opportunities: Being in the IT field, you'll likely have access to various learning resources. Use this to your advantage by expanding your knowledge in cyber security-related areas.

Networking:

Building relationships with colleagues and professionals in your organisation's IT department can open doors to mentorship and guidance in your cyber journey.

[BACK TO CONTENTS PAGE >](#)

EDUCATION & CERTIFICATION PATHWAYS: STAY RELEVANT BY STAYING CURIOUS

In the dynamic world of cyber security, characterised by perpetual advancements and evolving threats, a strong commitment to continuous learning is paramount. Establishing a foundational understanding of IT is crucial, and obtaining certifications, such as an IT fundamental certificate, serves as a solid starting point.

“

Learn, share, learn more, build, break, learn, fix, share, repeat.

(Survey Participant)

Our Roundtable Workshop echoed the unanimous sentiment in our survey that a strong aptitude for learning is indispensable in this field. The consensus highlighted a cyclical process of learning, sharing, building, breaking, fixing, and repeating. Delving into the fundamentals and compliance of cyber security was emphasised, urging individuals to take the time to thoroughly grasp these essentials.

While choosing a specific pathway is a personal decision, whether through tertiary education or certifications, both avenues demonstrate dedication to the industry and its ever-evolving landscape. While formal education provides a tangible metric for comparison during the hiring process, the survey highlighted that, particularly for junior team members, showcasing passion, energy, and an eagerness to learn also hold immense value.

“

Formal education does provide value in being able to easily compare individuals during the hiring processes. However, when it comes to junior team members the most value is showing passion, energy and enthusiasm to learn more.

(Survey Participant)

E2 CYBER & LUMIFY

We have established a formal relationship with Lumify for cyber training, a decision that has been based on a number of factors:

- 1. Australia's largest and most reputable IT and Cyber training organisation.**
- 2. The e2 Cyber team have completed certifications through onsite training conducted by Lumify and were impressed with the quality of trainers, the facilities, the organisation logistics on the day and the ongoing support.**
- 3. Their people. The Lumify team, from sales, to marketing trainers to practice leads are all great people who do truly care.**

Learning is a personal journey though and who you choose to train and learn with, is genuinely your choice.

[BACK TO CONTENTS PAGE >](#)

EDUCATION & CERTIFICATION PATHWAYS: STAY RELEVANT BY STAYING CURIOUS

Industry certifications, identified in the survey as the most relevant education path, offer a tangible demonstration of expertise. The advice is to embark on a structured journey, starting with a general security focus, followed by certifications like CompTIA+, before branching into a specialty such as GRC or Penetration Testing. The recommendation also advocates pairing certification pursuits with practical experience in an IT/Helpdesk role, providing a holistic approach to skills development and professional growth in cyber security.



POPULAR CERTIFICATIONS VOTED IN OUR SURVEY WERE:

- CISSP
- Cert IV Cyber security
- ISC2 Certified in Cyber
- CISM
- ISO Lead Auditor
- CompTIA A+, CompTIA Security+



ONLINE TRAINING PLATFORMS:

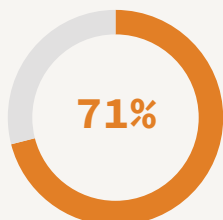
- [TryHackMe](#)
- [HackTheBox](#)
- [LinkedIn Learning](#)
- [Safer Internet Project](#)



[BACK TO CONTENTS PAGE >](#)

HOMELABS – SHOWCASE YOUR INTEREST IN THE TECH

A homelab is a personalised environment where individuals pursuing a career in cyber can experiment, learn, and apply various technologies and methodologies in a hands-on manner.



have/use a homelab or
free online training
platforms at home

It serves as a practical extension of formal education, allowing enthusiasts to bridge the experience gap that might exist on their resumes. Even for roles in Governance, Risk, and Compliance (GRC), a homelab demonstrates a genuine passion for continuous learning. Whether it involves setting up virtual environments, experimenting with cyber security tools, or participating in platforms like HackTheBox, a homelab showcases an individual's commitment to gaining technical proficiency. The networking opportunities within homelabs, such as engaging with communities like Reddit's r/homelab or Whirlpool Forums, are invaluable.

Understanding and applying frameworks become more tangible through hands-on experience. Ultimately, having a homelab not only enhances technical skills, but also demonstrates a proactive approach to staying abreast of evolving technologies, thereby making your CV stand out in the competitive field of cyber security.

“

Doesn't have to be expensive – or even a “lab” as such. It needs to be something that demonstrates that you're trying to learn the technical aspects of things.

(Survey Participant)



HOMELAB SUBSCRIPTIONS:

- [HackTheBox](#)
- [TryHackMe](#)
- [GNS3](#)

“

How am I supposed to learn and understand what's in the framework if I don't know how to apply them in the first place?

(GRC Consultant)



READ OUR HOMELABS BLOG:

HOMELABS: CYBERS SECURITY'S SECRET WEAPON FOR SKILL ENHANCEMENT & CAREER DEVELOPMENT

<https://www.e2cyber.com.au/homelabs-cyber-skill-enhancement-career-development>



[BACK TO CONTENTS PAGE >](#)

FRAMEWORKS – WHAT ARE THEY AND WHERE TO FIND THEM

A cyber security framework is a comprehensive and structured approach that organisations adopt to manage and enhance their overall cyber security posture. It serves as a strategic blueprint, providing a set of guidelines, best practices, and standards to help organisations identify, protect, detect, respond to, and recover from cyber threats and incidents. These frameworks are designed to be flexible and adaptable, allowing organisations to tailor their cyber measures to their specific needs and risk profiles. Commonly utilised frameworks include the NIST Cyber security Framework, ISO/IEC 27001, and CIS Critical Security Controls. By implementing a framework, organisations can establish a systematic and organised approach to safeguarding their information assets, ensuring the confidentiality, integrity, and availability of their data and systems in an increasingly complex and dynamic threat landscape.

“

Understand there are multiple frameworks and understand the value of different frameworks and how they apply. Reading them is education enough! It's free; download it, understand it.

(Survey Participant)

“

You need to understand one framework in depth to be able to understand others. Pick one, go really deep into actually implementing it and actually seeing what those controls mean in practice.

(Survey Participant)

FRAMEWORKS:

ISM

www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

PSPF

www.protectivesecurity.gov.au/

NIST

www.nist.gov/cyberframework

SOC2

<https://blog.rsisecurity.com/introduction-to-the-soc-2-control-framework/>

Mitre

<https://attack.mitre.org/>

APRA

www.apra.gov.au/information-security

SOCI

www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

[BACK TO CONTENTS PAGE >](#)

ROLE TYPES DECODED

CONTRACT VS PERMANENT (GRAD/INTERN) ROLES

For graduates or interns starting a cyber security career, contract and permanent roles both have their merits. The choice may depend on personal preferences, career goals, and the specific circumstances of the individual. Sometimes it just comes down to which opportunity presents itself first!

Contract Roles:

These can be advantageous for gaining diverse experiences quickly, building a network, and exploring different areas of cyber security. However, they may involve more uncertainty and require a proactive approach to securing the next contract.

Permanent Roles:

These provide more stability, benefits, and a structured path for career development. Graduates or interns in permanent roles may have the opportunity to grow within a company and establish themselves in the industry.

COMPARISON AT A GLANCE:

CONTRACT ROLE	PERMANENT ROLE
Fixed Duration: Contract roles are typically of a fixed duration, ranging from a few weeks to several months or even years. They are project-based or task-specific.	Job Security: Permanent roles provide more job security as they are ongoing positions. Companies invest in the long-term development of permanent employees.
Flexibility: Contractors often have more flexibility in terms of work hours and locations. They may have the opportunity to work on various projects with different companies.	Stability: Permanent roles offer more stability, and employees become integral parts of the company culture and long-term strategies.
Income: Contractors are paid a higher hourly or daily rate as compensation for not receiving paid leave and superannuation contributions.	Benefits: Permanent employees receive benefits such as paid leave and superannuation contributions which contribute to a more stable financial package.
Learning Opportunities: Contract roles can provide exposure to a variety of projects and technologies, offering a steep learning curve.	Career Development: Companies often have structured career development programs for permanent employees, including training, mentorship, and opportunities for advancement.

[BACK TO CONTENTS PAGE >](#)

ROLE TYPES DECODED

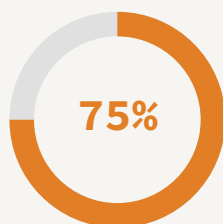
SALARY VS DAILY RATES:

Salary and rates fluctuate depending on demand and skillset in the market. We update our guide every quarter based on what we are seeing in the market:

Review our Salary and Rates Guide



www.e2cyber.com.au/salary-rate-guide



said they believe the government's push to enhance Australia's cyber posture is influencing more people to start a cyber security career.

PRIVATE VS PUBLIC SECTOR

Whether you start your career in the private or public sector, what is apparent is the industry belief that a significant number of individuals are drawn to cyber due to the government's efforts to enhance Australia's cyber security. When considering these career options, the choice between the public and private sectors often depends on the desired learning curve and career trajectory. Private sector roles are known for offering a steep learning curve, throwing professionals into the deep end, but providing invaluable hands-on experience. On the other hand, private sector tends to have a slower pace with lower expectations, allowing for a more manageable workload and opportunity to digest the scope.

Private sector opportunities in Canberra offer a unique advantage, as many private organisations deliver services to the government, providing professionals with the best of both worlds. Additionally, private sector employers often invest in training and mentoring programs, making it easier for individuals to enhance their skills.

However, it's crucial to note that certain cyber security roles in the public sector and those in the private sector providing services to federal government, particularly those related to intelligence, security, foreign policy or defence, may require security clearances, necessitating Australian citizenship, background checks and clearance procedures for interested candidates.

Learn more about AGSVA:



www.e2cyber.com.au/agsva-clearances

Ultimately, the decision between public and private cyber security careers hinges on personal preferences, career goals, opportunity and the type of work environment expected to be most conducive to professional growth. However, similar to deciding between a contract or permanent role, sometimes the choice is made by which opportunity you manage to secure first.

[BACK TO CONTENTS PAGE >](#)

CODE SHIFT – MAKING A CYBER CAREER CHANGE

With an increased demand for cyber skilled professionals, the projected earning potential, the interest in the mission of cyber security and because cyber encompasses so many fascinating areas, we see many candidates seriously considering cyber security as a relevant career change, with many pursuing the opportunity. Making any career change brings unique challenges, and every situation is different. We recommend asking yourself these key questions and exploring the options:

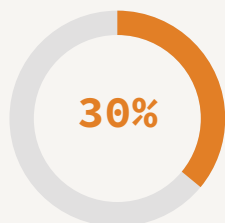
- Why cyber security?
- What skills are transferable?
- Where are your skills gaps?
- What will you do to learn and develop the required skills?
- Is this move financially viable?
- Do you truly know what a career change path will be?
- Have you sought real cyber career advice? A mentor can be invaluable!
- Do you have the support of your family/friends?
- Are you mentally and emotionally ready to undertake this journey?

More often than not, a pay cut/reduction will occur at the start of your new cyber career journey. This is something to be aware of and seriously consider as it can be the deciding factor as to why people don't pursue the career change. While the potential reduction in earnings is very likely to be short-term, knowing this at the start of the process will ensure you don't waste time or money on upskilling if this is not viable for your personal circumstances.



[BACK TO CONTENTS PAGE >](#)

JOIN THE CYBER COMMUNITY: BE AN ACTIVE NODE



said networking was essential to securing a role in cyber.

The cyber security community hosts a plethora of events, ranging from international conferences to local gatherings and webinars, making it easy to be an active member.

With 30% of our survey participants viewing networking as vital for securing a role in the industry, it is essential to embrace the opportunity to connect with professionals in the field. Likewise, seeking mentorship was highlighted as invaluable, not just for those starting out, but at every stage of your career in cyber security.

Participating in networking and community events not only enhances your cyber knowledge, allowing you to learn from seasoned professionals' experiences, but also keeps you updated on industry trends necessary for professional advancement. Networking emerges as a pivotal skill for those venturing into a cyber security career, providing abundant opportunities for learning and personal growth. It's essential to explore diverse communities within the field, some focusing on technical aspects while others emphasise networking. Following advice to explore various niches in the early stages helps in identifying personal interests and strengths.

“

Networking with the community is the most important skill to have when starting out.

(Survey Participant)



AUSTRALIA CYBER EVENTS:

- AISA/ CyberCon
- SecTalks
- CrickeyTalks
- AustCyber
- ASWN
- Azure meet ups
- AWS meet ups
- Vets in Cyber

“

Come in, get around to a whole bunch (of events) and understand what you like. They're all different, some technical, some networking. There are some very niche ones - try lots in your first few years and pick the ones you like.

(Survey Participant)

[BACK TO CONTENTS PAGE >](#)

NEURODIVERSITY IN THE DIGITAL CORTEX

There is a growing recognition of the unique strengths and perspectives that neurodivergent individuals bring to the table, such as their unique perspectives and problem-solving abilities that can enhance a team's ability to identify and mitigate cyber threats.

Organisations are actively working to create inclusive environments and flexible arrangements that support and encourage neurodiversity in cyber security careers.

Recognising the diverse talents that neurodivergent individuals possess, employers are implementing inclusive hiring practices to make such candidates feel comfortable, and are fostering a culture of acceptance.

“

Back yourself. If you think you know your stuff, back yourself!

(Survey Participant)

Specialised training programs and mentorship initiatives tailored to accommodate different learning styles are being developed to ensure that neurodivergent professionals receive the necessary support to excel in their roles. By embracing neurodiversity, the cyber security industry not only benefits from a broader pool of innovative thinkers, but also reinforces the notion that diversity in thought and approach is a key asset in safeguarding digital landscapes.

“

Get involved and ride the rollercoaster. There's a spot for everyone.

(Survey Participant)



[BACK TO CONTENTS PAGE >](#)

UNLOCK YOUR DIGITAL DISTINCTION TO STAND OUT

When pursuing a cyber security career, you need to put your best foot forward to stand out! Crafting a meticulously detailed CV is paramount. Ensure it highlights not just your technical skills, but also your problem-solving abilities, certifications, and relevant coursework or projects. Additionally, industry experience, even through internships or part-time roles, adds immense value. Detail any hands-on work you've done, whether it's analysing malware or conducting penetration testing.

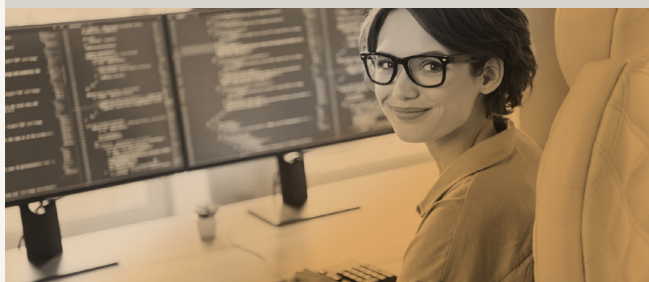
As we've highlighted, cyber security has a strong community and networking focus, so demonstrating participation is equally vital; engage in cyber security forums, attend conferences, or contribute to open-source projects. Demonstrating your commitment to continuous learning and collaboration not only showcases your passion for the field, but also your ability to work effectively within a team.



READ OUR BLOG:

ACCELERATE YOUR CAREER – JUNIOR CYBER SECURITY CONSULTANTS

www.e2cyber.com.au/accelerate-your-career-junior-cybersecurity-consultants



CV AND COVER LETTER

It's important to include experiences that might not immediately seem relevant on your CV, such as part-time work while you've been studying. These often demonstrate valuable traits, such as: character, customer service skills, and adaptability to fast-paced environments. Additionally, a thoughtfully crafted cover letter can complement your CV by highlighting your interests, and explaining how they align with the role you're pursuing. Avoid generic cover letters; instead, tailor each one to the specific job you're applying for to showcase your intentions and aspirations effectively, and how they relate to that particular role.

Download our CV template



www.e2cyber.com.au/cyber-cv-template

After landing a position, keep your CV up to date by listing the top five accomplishments from each role, so you don't forget the specifics of what you've achieved.

SHARPEN COMMUNICATION SKILLS

Clients are always interested in "soft" skills. Develop strong communication and problem-solving skills, and the ability to effectively communicate security issues to both technical and non-technical stakeholders, is crucial in the cyber security profession.

STAY INFORMED:

Stay updated on the latest cyber security trends, threats, and technologies. Subscribe to industry publications, blogs, and follow cyber security experts on social media platforms to stay informed on the rapidly evolving landscape.

[BACK TO CONTENTS PAGE >](#)

UNLOCK YOUR DIGITAL DISTINCTION TO STAND OUT

INTERVIEW PREPARATION

When preparing for an interview, it's crucial to prioritise storytelling over simply listing certifications. Show your passion! Sharing stories about your experiences and achievements resonates far more than a mere recitation of qualifications. A standout factor in interviews is the demonstration of practical skills through homelabs.

When asked, "How do you learn?" seize the opportunity to showcase your homelab setup. Delve into why you have it, what projects you're running, and what you're learning from it. Engaging in hands-on learning, and demonstrating enthusiasm, can truly distinguish you during the interview process.

“

If you want to do that job, then show you're excited about it.

(GRC Consultant)



Access our interview preparation docs



www.e2cyber.com.au/interview-prep



READ OUR BLOG:

CRACK THE CODE TO CYBER INTERVIEW SUCCESS

www.e2cyber.com.au/crack-the-code-to-cyber-interview-success



[BACK TO CONTENTS PAGE >](#)

UNVEILING THE POWER OF CYBER SPECIALIST RECRUITERS

Working with a specialist cyber recruiter can streamline your job search process and increase your chances of successfully landing a role in cyber security. While we might not have a large number of entry level roles listed, we are constantly connecting with Australian private and public organisations, and know when they are taking in their next cohort of cyber juniors.

Sign up for job alerts:

 www.e2cyber.com.au/job-alerts#JobAlerts

Follow us on LinkedIn

 www.linkedin.com/company/e2-cyber

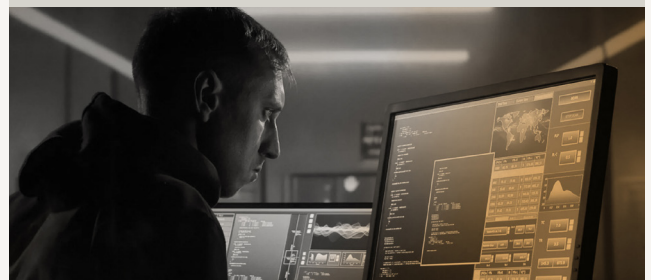
Once you've landed your first role, there are many benefits of working with a specialist cyber recruiter, read more in our blog.



READ OUR BLOG:

WHY WORK WITH A CYBER SPECIALIST RECRUITER

www.e2cyber.com.au/why-work-with-a-cyber-specialists-recruiter



CHAT TO US TO FIND OUT MORE



1300 072 097



contactus@e2cyber.com.au



www.e2cyber.com.au



[BACK TO CONTENTS PAGE >](#)