The Decipher Bureau

Australian Cyber Security

Salary Guide 2022

Introduction

Welcome to the Decipher Bureau's 2022 Annual Cyber Security Salary Guide. Each year we collate this comprehensive report to provide professionals and businesses with data and analysis on current employment and hiring trends within the Australian cyber security industry.

The insights in this guide have been put together by The Decipher Bureau over the past 12 months whilst recruiting exclusively for Australia's Cyber Security and Technology Risk market.

Our team of experienced recruitment professionals work with the cyber security community across Australia. Our clients range from ASX listed and Fortune 500 businesses, through to niche cyber security consultancies. Our network of professionals work across the spectrum of roles in cyber security and technology risk.

We hope you find this guide informative and useful – whether you are looking for new opportunities or seeking to hire talent in this dynamic sector.

For a confidential discussion with an experienced recruiter please reach out to any of our consultants. Further information and contact details can be found on our website: www.decipherbureau.com

Notes:

Junior – 0-3 years experience in role

Mid – 3-6 years experience in role

Senior – 7 years + experience in role

Specialist denotes qualified and experienced professional in this field.

Some salaries for security professionals may fall below or above those listed in this guide.

*Sales – Bonus can make up a substantial part of package – Bonus levels between vendors and consultancies / MSP's can vary significantly.

N/A - Not enough data or no contract requirements in this area.

Salaries are inclusive of superannuation only. The salaries listed do not include bonuses, allowances, training etc.

The Decipher Bureau Australian Cyber Security Salary Guide 2022

Role	Salary (000's incl super)		Day Rate (8 hours incl super)	
CISO - SME	$300+		N/A	
CISO - Enterprise	$400+		N/A	
Head of / Practice Lead	$220	$280	N/A	
Security Manager / SOC Manager	$210	$260	N/A	
Security Architects - Mid	$170	$200	$800	$1,000
Security Architects - Senior	$195	$250	$1,100	$1,450
Cyber Risk / GRC - Junior	$80	$110	N/A	
Cyber Risk / GRC - Mid	$110	$160	$750	$1,000
Cyber Risk / GRC - Senior	$160	$220	$1,000	$1,300
Security Analyst - Junior	$70	$90	N/A	
Security Analyst - Mid	$90	$150	N/A	
Security Analyst - Senior	$150	$210	N/A	
DFIR Specialist	$180	$250	N/A	
Threat Intelligence Specialist	$150	$200	N/A	
Security Engineer - Junior	$70	$100	N/A	
Security Engineer - Mid	$100	$150	$650	$850
Security Engineer - Senior	$160	$200	$800	$1,100
SIEM Engineer	$140	$200	$900	$1,200
DevSecOps Engineer	$160	$220	$900	$1,200
Cloud Security Engineer	$150	$200	$900	$1,200
Penetration Tester - Junior	$70	$110	N/A	
Penetration Tester - Mid	$110	$170	$750	$1,000
Penetration Tester - Senior	$170	$210	$1,000	$1,250
Red Teamer	$180	$220	N/A	
Application Security Specialist	$140	$200	N/A	
Cyber Security Business Analyst	$120	$170	$900	$1,200
Cyber Security Project Manager	$170	$220	$1,000	$1,500
Service Delivery Manager	$150	$200	N/A	
IDAM / PAM Engineer	$110	$170	$800	$1,000
IDAM / PAM Consultant	$150	$190	$900	$1,200
Security Awareness Specialist	$135	$220	N/A	
Cyber Security Pre-Sales	$180	$235	N/A	
Cyber Security BDM*	$165	$240	N/A	
Cyber Security Account Manager*	$140	$180	N/A	

Disclaimer: The data provided in this guide is sourced from information gained by The Decipher Bureau over the past 12 months recruiting exclusively for Australia's Cyber Security and Technology Risk market. We believe this data provides an accurate representation of the current state of play in Australia. Salaries will vary depending on industry sector, location, accreditations and years of experience. Analysis and review of this data are our own views. This information is offered as a guide only and may not reflect other benefits offered by companies such as training, certifications, bonuses and shares. The Decipher Bureau do not hold any liability for the accuracy of this information.

State of the Market

It will come as no surprise that the trend of salary increases across the cyber security sector continued into the 2021 / 22 financial year.

In fact, it would appear this market is booming - we have seen a larger growth in salaries than in previous years, with average increases of around 15% over the past 12 months (and in some niche areas, salaries have increased by up to 25%).

This year has been a real battle for companies to secure and retain top talent. Certain skills have been in high demand and this, combined with a real shortage of available talent, has driven up salaries and expectations

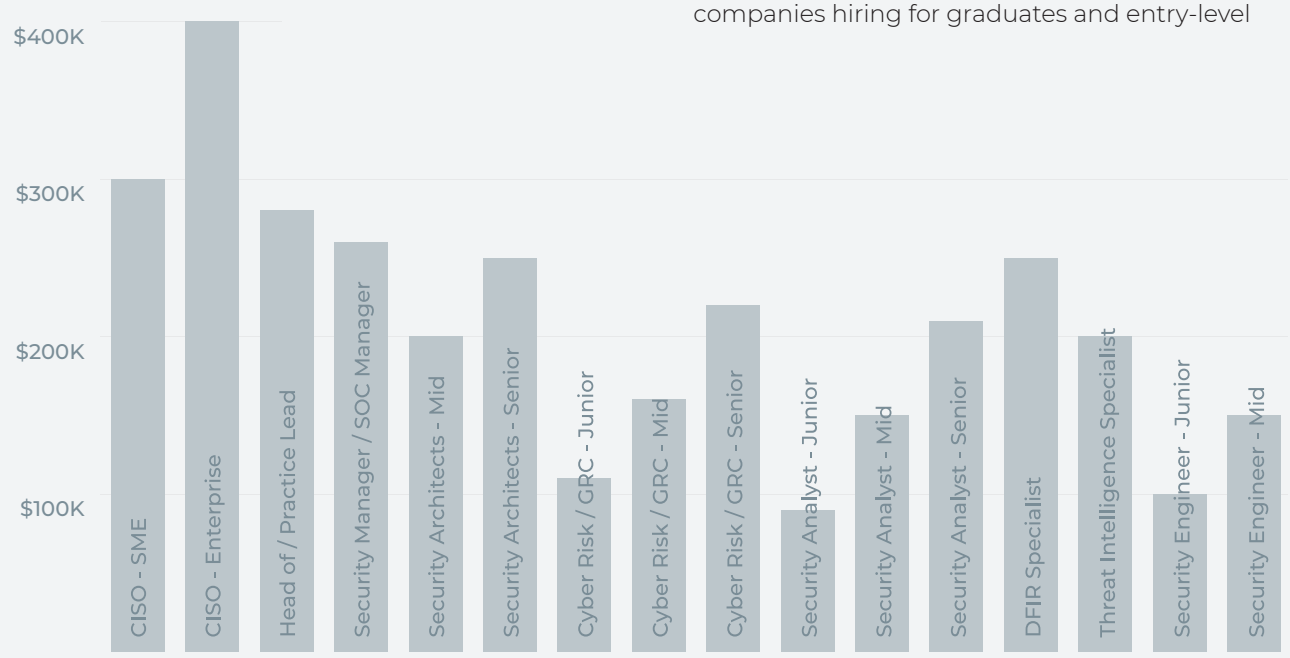
To either attract or retain, companies are needing to make their offering increasingly attractive, whether it be through salaries, flexibility, culture, interesting work, training, work life balance and/ or career progression.

Salaries have experienced average increases of 15% over the past 12 months (and in some niche areas, salaries have increased by up to 25%)

In addition to COVID restrictions preventing travel, incoming talent from overseas has been slowed due to delays in permanent residency grants and costly 482 Visas which are time consuming and labour intensive to apply for.

However, in the wake of the pandemic, and with increased awareness of salaries and bargaining power in the current climate, we've seen local talent being more open to hearing about new opportunities. Contractor daily rates have also risen in most areas and this, combined with increased confidence in the market, has meant that some professionals have also been willing to leave permanent positions to take up high-paying contracts.

We hope that the next year will see more companies hiring for graduates and entry-level



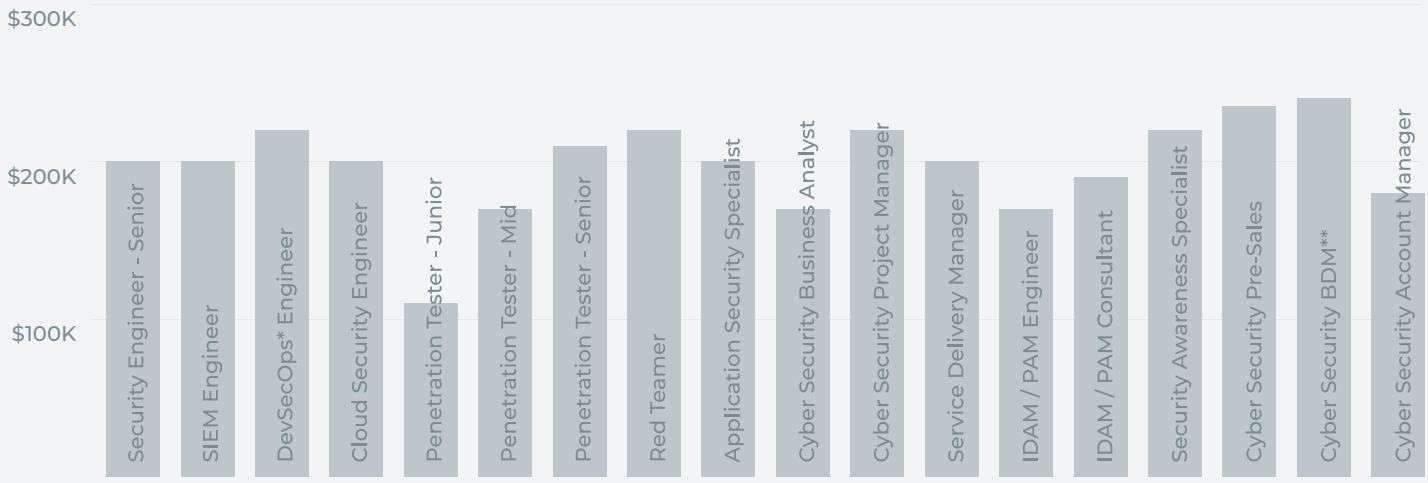
roles, as well as people looking to transition into a cyber security role from other technical positions. There is also a real need to increase diversity in the industry. We are hopeful that proposed visa changes will make it easier for organisations to hire talent on sponsorships, to encourage skilled professionals from overseas to move to Australia and subsequently strengthen the local technology market.

In 2020 there were increased requirements for security operations and Governance, Risk and Compliance (GRC) roles. In contrast, this past year has seen interest develop across all disciplines with a strong increase in demand in DevSecOps, Application Security, Incident Response and Threat Hunting. Unlike the previous 12 months, this last financial year has seen consistent recruitment across all locations.

We are also seeing hiring decisions that were put on hold well and truly active again. Many organisations have increased headcount by up to 30%, and we anticipate a continued level of opportunity in the 2022/23 financial year.

Other activity we've noted in the market over the past financial year include:

- A significant increase in investment in security by many companies, resulting in hiring additional headcount for BAU roles and projects.
- An increasing number of senior roles with more appropriate salaries attached for "Heads of" positions
- Companies increasing salaries for existing employees as a retention strategy
- Counter offers from employers becoming more common in a bid to keep staff from leaving
- Continued M&A activity, with a number of boutique Australian companies being acquired by larger players or merging with other boutiques.
- Further regulation and compliance e.g. The Critical Infrastructure Bill which has increased the need for governance across many industry sectors.



Work/Life after COVID

Over the last year we've seen a steady flow of staff starting to move back to the office, with most organisations now operating a hybrid model (particularly in Brisbane and Canberra - Sydney and Melbourne have moved more cautiously, with many still skewed towards working from home). Vaccine mandates also impacted staff in some industries, however we expect this to lessen over the next 12 months. In-person events have started to kick off again, with cyber-specific conferences and meet-ups mostly back up and running.

In a number of cases, the previous two years have highlighted an organisation's ability to work 'remote first', giving employees the opportunity to be 'work from home' (WFH) full time - and removing the need for candidates to be location specific when hiring.

As a result of these new ways of working, and to counteract 'the Great Resignation', talent acquisition now needs to be slick and efficient.

It is now not unusual to undertake 2-3 interviews within a fortnight, and verbal offers to be formalised within 1-2 days.

The War for Talent

We continue to see that salary alone is not enough to secure talent - Employee Value Propositions (EVPs), bonuses, and benefits are becoming an increasingly important component of employment packages for cyber security professionals.

As a result of these new ways of working, and to counteract 'the Great Resignation', talent acquisition now needs to be slick and efficient.

Just as is the case with base salaries, bonuses can vary significantly between organisations and sectors. Some examples are provided below:

- Boutiques and Systems Integrators can pay 5-15% bonuses (% calculated on base)
- Large enterprise typically pay 10-30% bonuses (% calculated on base)
- Security Software Vendors typically pay:
  - Sales Engineers 70-80% base and 20-30% commission, plus superannuation
  - Sales Executives 50% base and 50% Commission, plus superannuation.

Other benefits we see as part of an employment package include:

- Health insurance and car allowances (fully subsidised health insurance being more common in US companies)
- Tech allowances for companies operating a 'bring your own device' (BYOD) model
- Various corporate discounts such as health insurance, gym membership, mobile phone, travel, childcare, etc.
- Extended Maternity and Paternity leave and childcare support
- Salary sacrificing
- Vehicle novated leasing
- Ability to earn more annual leave
- Financial support for setting up a WFH space

Migration & Visas

Due to the pandemic, the last two years have seen a significant reduction in migration to and from Australia. We are anticipating this to change significantly in the coming years. With the State borders opening, combined with more roles being able to be done remotely, we have already witnessed an increase in interstate movement.

International borders are now open in varying degrees, but we're only starting to see a trickle of migration and workforce arriving – mostly those who already possessed their own visas e.g. a Distinguished Talent Visa. Companies are still showing a reluctance to go down the sponsorship route, most likely due to cost (financial and time) and risk. The conversion or extension of student visas has created some opportunities for those looking to hire graduate/ junior roles. Additionally, the visa changes as of July 1 2022 may open up new pathways for skilled overseas candidates to gain permanent residency, thereby making the move to Australia more feasible and attractive.

Security clearances still tend to restrict opportunities in Canberra. Whilst some government organisations are building out teams across Australia, these still require a security clearance from the Australian Government Security Vetting Agency (AGSVA).

"This past year we have seen a notable shift in how businesses successfully recruit. Those who approach recruitment with a "how can we attract the candidate?" mentality, as opposed to assuming every candidate wants to work for them, are getting the best results. "

Matt Dunham
MANAGING DIRECTOR

Training / Development / Certifications

It is positive to see graduate and entry-level recruitment is back in full swing, as well as universities and government departments developing internship programmes with cyber security companies. This highlights a continued need for mentors in this area, and there are an increasing number of experienced security practitioners who offer mentoring. The Decipher Bureau “Connect” is one initiative that aims to connect jobseekers to mentors in the industry. “Connect” was successful at AusCert and CrikeyCon, and we aim to roll it out at other cyber events. Organisations such as The Tech Girls Movement are another fantastic initiative to help the community to continue to grow.

For employee professional development, most companies have training budgets ranging from $3,000 - $10,000. In recognition of the need to create a wider talent pool, some companies have programmes to retrain / upskill staff in specific areas of need, and we are seeing an emergence of specialist training providers (including within the cyber industry) being engaged by large enterprises.

In terms of Certifications we have seen most demand for:

- CISSP
- OSCP
- SANS GCIH (Incident Handling)
- SANS GCFA (Forensic Analysis)
- ISO27001 Lead Auditor / Implementer
- CCSP
- CCSK
- CISM
- SABSA
- AWS or AZ500 (cloud security)
- CompTIA Security+
- GIAC Information Security Fundamentals (GISF)

Costs for these range significantly.

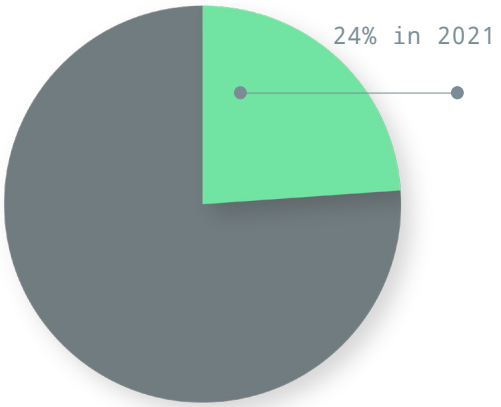
Diversity & Inclusion

The global 2021 (ISC)² Cybersecurity Workforce Study surveyed certified cyber security professionals in official cyber security functions as well as IT/ICT professionals who spend at least 25% of their time working on cyber security responsibilities. They found that globally, women working in cyber security currently account for about one quarter (24%) of the overall workforce. This is a significantly higher finding than from 2017, when only 11% of study respondents were women (it should be noted that the 2021 study used a revised research methodology, which likely accounts for the larger representation of women).

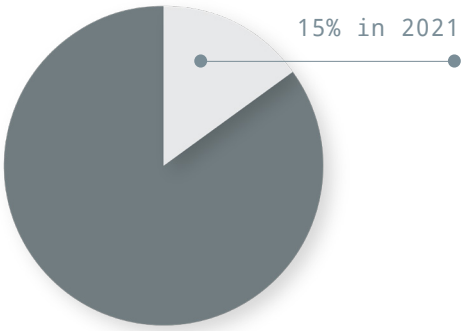
Despite still being significantly underrepresented, there appears to be a shift in the right direction, with the report also observing a higher percentage of women in cyber security achieving C-level roles. It also lent weight to the argument for organisations to look at upskilling current staff or looking for more diverse experience to fill cyber security roles - alternate points of entry are more common for women than men (only 38% of female participants started their careers in IT compared to 50% of male participants).

In Australia there doesn't appear to be a definitive number on the percentage of women in cyber security, however recent reports suggest the number is less than 15% of the sector.

We believe that thanks to the great work by organisations such as AWSN and the Tech Girls Movement (and others), the number of women in cyber security will continue to rise in Australia. There is no doubt more work needs to be done on this and other areas of diversity to ensure



Percentage of women in the global cyber workforce.



Percentage of women in the Australian cyber workforce.

that the Australian cyber security sector has a fully inclusive workforce. This is vitally important for the profession as the number of cyber security jobs available continues to rise. Moreover, it's imperative that these roles are filled by a diverse workforce from different backgrounds whose experience and perspectives give organisations a more innovative approach to tackling cyber solutions and an improved company culture.

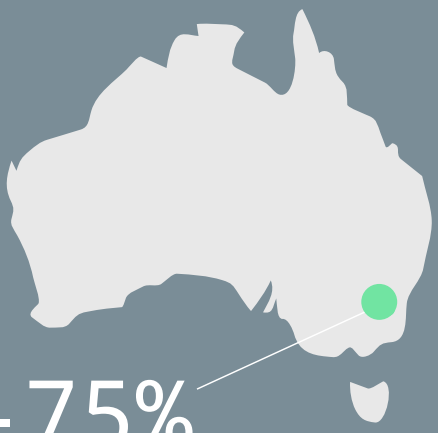
The Decipher Bureau will continue to support fantastic initiatives such as AWSN, VetsinCyber and TechGirls Movement.

Spotlight on Canberra

Over the years, Canberra has always been a very competitive market for cyber security resources and last financial year was no exception. Owing to the concentration of government agencies there, and the need for security clearance, the much higher earning potential for 'cleared' skilled resources to work as contractors means it's become increasingly difficult to hire permanent talent. Contractor rates have also increased, and it is not uncommon to see workers who were in a permanent role move to a consulting engagement for a 35-75% higher annual gross income.

Even as immigration increases this will not affect the shortage of cleared skilled resources so we expect the ACT market to remain competitive, and for permanent salaries and contractor rates to continue to rise.

One point of note is that more federal government agencies are opening up opportunities across the states which will no doubt help ease the pressure. Whilst salaries in industry and consulting are attractive, government roles offer great training & initiatives. The government are doing a great service in increasing the talent pool and helping bring the next generation of cyber talent through.



35-75%
higher income
for consultants per annum

Rise of the Digital Security Specialist

As more and more of our purchases are made online via e-commerce applications, the digital threat landscape increases and therefore so too does the need for improved application security. We are being asked to search for SecDevOps Consultants, AppSec Engineers, Digital Security Specialists, and a number of variations of a similar theme. As organisations develop at pace and in the cloud, the need for resources with experience of security in a devops and cloud environment is going through the roof.

There are only a finite number of skilled resources with this experience so companies will need to retrain staff, move site reliability engineers across to this area of cyber or bring on cloud-native graduates and help them to upskill swiftly.

Leadership Roles

Over the past 12 months, Australia's ASX Top 50 companies have experienced their fair share of cyber security challenges. As a result, Chief Information Security Officers (CISOs) at the big end of town are in the spotlight like never before. The pandemic has accelerated digital transformations in many large enterprises, bringing with it exposure to more threats. Remote working has created endpoint concerns with employees working from home with less supervision and fewer technical controls. Governments and regulators are also demanding stronger security requirements for critical infrastructure and systems of national significance.

Given the serious nature of the current threat landscape, combined with shareholders demanding peace of mind, and the potential brand/reputation damage that accompanies a high-profile breach, the majority of ASX Top 50 companies (over 80%) have committed to a dedicated CISO. We have also witnessed the emergence of Deputy CISO roles focusing on day to day management of teams well as a significant increase in "Head of" roles leading specific technical capabilities.

The remaining 15-20% of Australia's largest organisations have other arrangements in place or have someone wearing multiple technology hats (cyber security being one).

From a diversity perspective we previously noted the Australian cyber security industry has a female participation rate of approximately 15%, but this drops to nearer 10% for female CISOs across our 50 largest corporations. Whilst base salaries for CISOs may range from $300K to $500K, anecdotal feedback from the market also suggests that a number of big corporate CISO salary packages now stretch into the seven figure range overall, with more likely to join this group in 2023.

Security Operations

As was the case last year, security operations teams continued to grow and diversify, with more service providers offering managed SOC solutions. We are seeing that roles continue to be more defined e.g. L1, L2, Incidents Response (IR), Threat Hunting, Security Automation, SIEM Engineering.

We also noted a particularly high demand for Incident Response and Threat Hunting professionals over the past 12 months, with many companies in bidding wars to attract key individuals.

Cyber Risk & GRC

Demand for Governance, Risk and Compliance (GRC) professionals continued at all levels; with most coming from within the consulting field in response to an increased requirement for these roles to provide strategic advice.

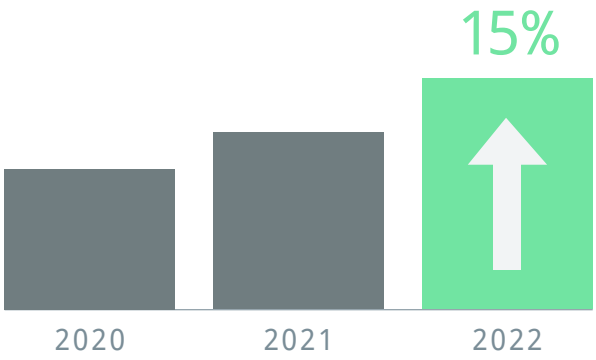
We expect that the demand is unlikely to slow due to the rise in governance led strategies within organisations, implementations of ISO27001, NIST and Essential 8 frameworks and/or the build and roll out of Information and Security Management Systems (ISMS)

Offensive Security

There has also been continued demand for penetration testers and red teamers (the CORIE framework still driving the demand for red team engagement), with more companies bringing these roles in-house.

Salaries have increased for professionals in this area, however a major draw for penetration testers when switching jobs is the nature of the work. Red teaming, proper adversarial simulation, physical security attacks (black teaming), and the chance to perform security/ malware research make opportunities more attractive. Because of this, many testers are interested in working with smaller, highly specialised businesses where they can get involved across the scope of work, instead of large corporates.

In terms of career development, for entry-level roles the OSCP continues to be the gold standard certification.



Salary averages are up 15% in the past year

OT Security

Over the past few years there has been ongoing investment and awareness to address Operational Technology (OT) security challenges. This could possibly be due to an increase in maturity within organisations, as well as a greater understanding of risk profiles, but is more likely a result of the Critical Infrastructure Act which came into force in 2018, but became much broader in its scope at the beginning of 2022. The major infrastructure projects over the past decade have created work – and notably the lifecycle of the projects are long and now getting to a point when cyber teams are needed to analyse risk and implement controls. This has created a continued rise for OT skills and possibly even doubled the demand for OT security specialists.

IDAM / PAM

Identity and Access Management (IAM) skills remain in very high demand as organisations need to ensure their IAM solution is fit for their cloud platform in post-COVID working conditions. We've seen identity become increasingly important when organisations go through a digital transformation journey with the need to factor in working from home and flexible working arrangements.

There are a handful of global vendors who dominate the market in Identity and Access Management and Privilege Access Management, with demand for their products and the people who can implement the solution as high as we've seen. As a result, salaries have been driven up by the shortage of available talent, particularly those with deep technical product knowledge in one of these key vendors.

Notably, a large pool of these skilled candidates are in professional services, consultancies and vendors, more so than in industry. Some larger enterprises have built out their IAM capability but most companies have to use external services to design and implement the solutions. The market is also heavily reliant on talent from overseas who either obtained skilled permanent residency or are on 482 sponsorships.

Contract & Temporary Workers

Contract rates remain buoyant, and in many cases we have seen them rise to attract top talent. As touched on before, the higher earning potential of contracting has been a significant drawcard for permanent employees to consider making the switch (creating a challenge for organisations, the majority of whom prefer to secure permanent hires).

As in previous years, there continues to be the highest demand for contractors in Canberra, followed by Sydney. Organisations are likely to utilise overseas candidates to fill many of these roles as skilled immigration numbers pick up.

Summary

2021/2022 surpassed all expectations in terms of job opportunities, the talent shortage and movement of people. It has certainly been a job-seekers market, and a fantastic time for those looking to change careers or take advantage of the offers companies are willing to make to secure top talent. On the flip side, this has created a challenging market for employers, who will need to take stock of ways to retain current employees, as well as put their best foot forward to attract new staff in a highly competitive climate. As a community we will need to continue to drive initiatives that will bring more diversity and more talent into this exciting and dynamic industry.

Forecast / Outlook

Looking forward, demand for talent remains strong despite the economic headwinds. As Australia's cyber security industry continues to mature, we foresee similar levels of activity in the recruitment market for at least another 6-12 months. This in part will most likely be satisfied by an increase of overseas candidates, which may also stabilise the trend of ever-increasing salaries.

Companies are increasingly realising that they cannot hire all the capability they need with the current talent shortage. To combat this they will have to look at hiring junior to mid-level resources as well as developing the talent from within.

We also anticipate further spotlight on cyber security, with the appointment of the new Minister for Cyber Security. It's the first time cyber security has had its own portfolio in Australia's cabinet, highlighting the increasing importance placed on this function for both Government and businesses (as well as a positive step for diversity and gender balance by appointing a woman into the ministerial position).

The future looks bright for Australia's Cyber Security Sector. Despite minor challenges the industry remains dynamic and buoyant and will no doubt continue to produce fantastic opportunities for all involved over the coming years.

In this market, jobseekers can pick and choose, and typically receive multiple job offers. Companies with clear propositions, attractive salaries, robust benefits and flexibility are the ones attracting the best talent."

Paul Jenkins
DIRECTOR

About The Decipher Bureau

Established in 2014, The Decipher Bureau is Australia's leading Cyber Security and Technology Risk recruitment company.

With 8 specialist consultants and dedicated offices in Brisbane, Sydney and Melbourne, we have helped 100's of clients with specialist recruitment and temporary workforce solutions across Australia and South East Asia. We are passionate about the industry and actively participate in and support industry associations, events and conferences such as AISA, Girls in Tech, AWSN, Veterans in Cyber, CrikeyCon and BSides.

Looking to hire? We can provide market insights and help you access hard to find talent. Looking for a move? We can provide career advice and connect you with some of the best opportunities in Australia.

For further information and contact details please visit www.decipherbureau.com