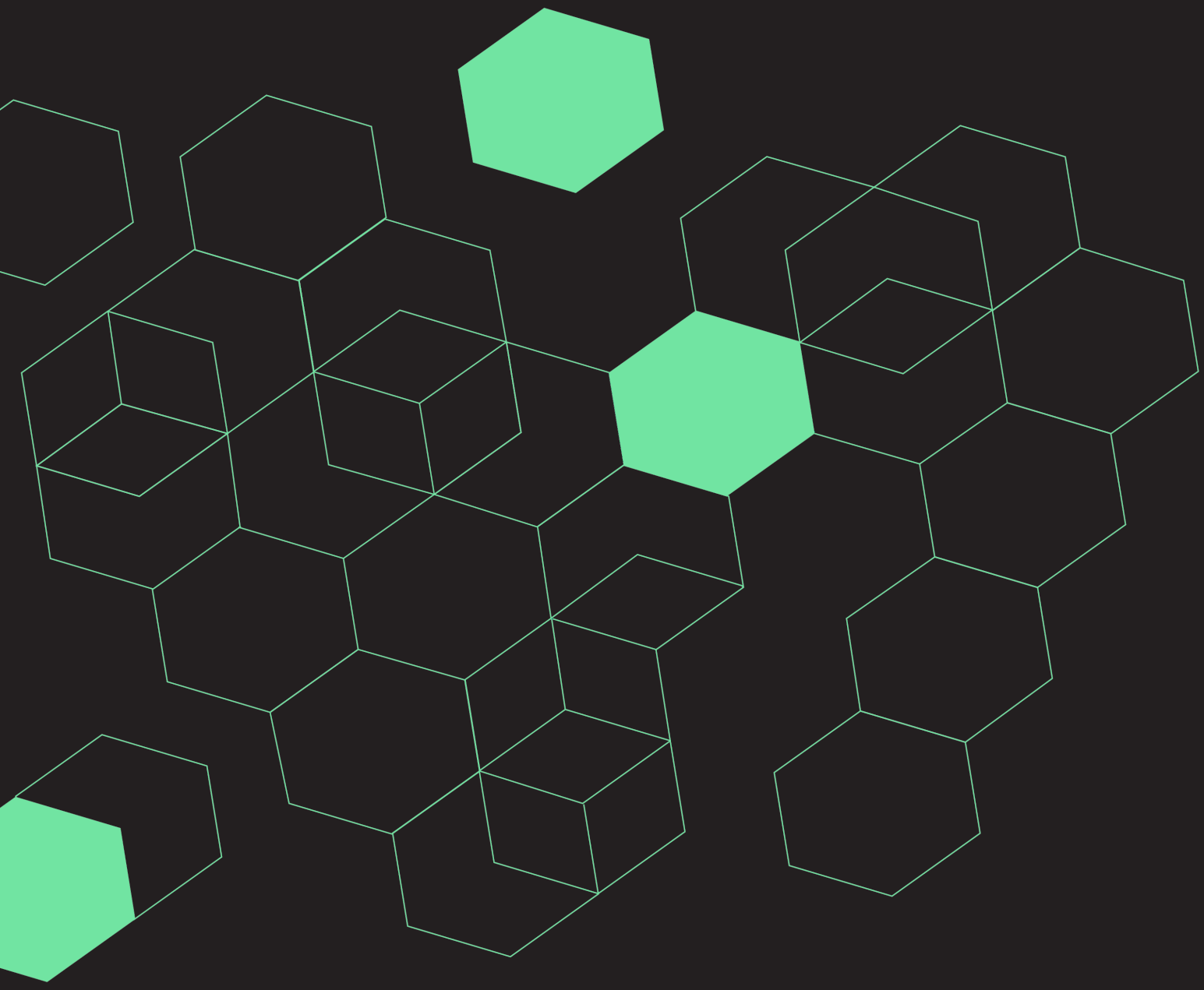
Decipher Bureau



The Decipher Bureau Australian Cyber Security Salary Guide 2021

Introduction

Welcome to The Decipher Bureau's 2021 Cyber Security Salary Guide. Each year we collate this report to provide businesses and job seekers with data on current employment trends within the Australian Cyber Security industry.

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

Because our consultants typically work with clients and candidates in major Australian cities, our data is most relevant to the eastern seaboard cities of Sydney, Melbourne and Brisbane. Salaries for Canberra's contract market are on average around 20% higher than the depicted data, with permanent salaries in the capital creeping slightly higher than those listed. This is due to strict requirements for security clearances and a gross undersupply of talent in the nation's capital.

We hope you find this guide useful and informative - whether you are looking to hire talent in this dynamic sector or considering a change yourself.

For a confidential discussion with an experienced recruiter please reach out to any of our consultants. More 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
Some salaries for security professionals may fall below or above those listed in this guide.
*Incident Response Specialist - Includes Threat Hunting & Digital Forensics
**Security Engineer - Includes Network, Cloud & SIEM Engineers
***DevSecOps - Includes SOAR Engineers
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 2021

Role	Base Salary (000's incl super)		Day Rate (8 hours incl super)	
CISO - SME	$220+		$1,500+	
CISO - Enterprise	$320+		$2,000+	
Head of / Practice Lead	$200	$250	N/A	
Security Manager / SOC Manager	$190	$250	N/A	
Security Architects - Mid	$150	$175	$800	$1,000
Security Architects - Senior	$175	$230	$1,000	$1,300
Cyber Risk / GRC - Junior	$70	$100	N/A	
Cyber Risk / GRC - Mid	$100	$140	$750	$900
Cyber Risk / GRC - Senior	$140	$200	$900	$1,200
Security Analyst - Junior	$65	$90	N/A	
Security Analyst - Mid	$90	$140	N/A	
Security Analyst - Senior	$140	$200	N/A	
Incident Response Specialist*	$160	$220	N/A	
Security Engineer - Junior	$65	$100	N/A	
Security Engineer - Mid	$100	$140	$650	$850
Security Engineer** - Senior	$140	$180	$800	$1,100
DevSecOps*** Engineer	$150	$200	$900	$1,200
Penetration Tester - Junior	$65	$90	N/A	
Penetration Tester - Mid	$90	$140	$750	$1,000
Penetration Tester - Senior	$140	$190	$1,000	$1,250
Red Teamer	$180	$220	N/A	
Application Security Specialist	$120	$180	N/A	
Threat Intelligence	$145	$185	N/A	
Cyber Security Business Analyst	$110	$160	$800	$1,100
Cyber Security Project Manager	$160	$200	$1,000	$1,500
IDAM / PAM Technical Specialist	$110	$170	$600	$1,000
Security Awareness (Non-Technical)	$100	$140	N/A	
Security Awareness (Technical)	$120	$170	N/A	
Cyber Security Pre-Sales	$160	$225	N/A	
Cyber Security Inside Sales	$75	$110	N/A	
Cyber Security Sales	$150	$250	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.

Analysis

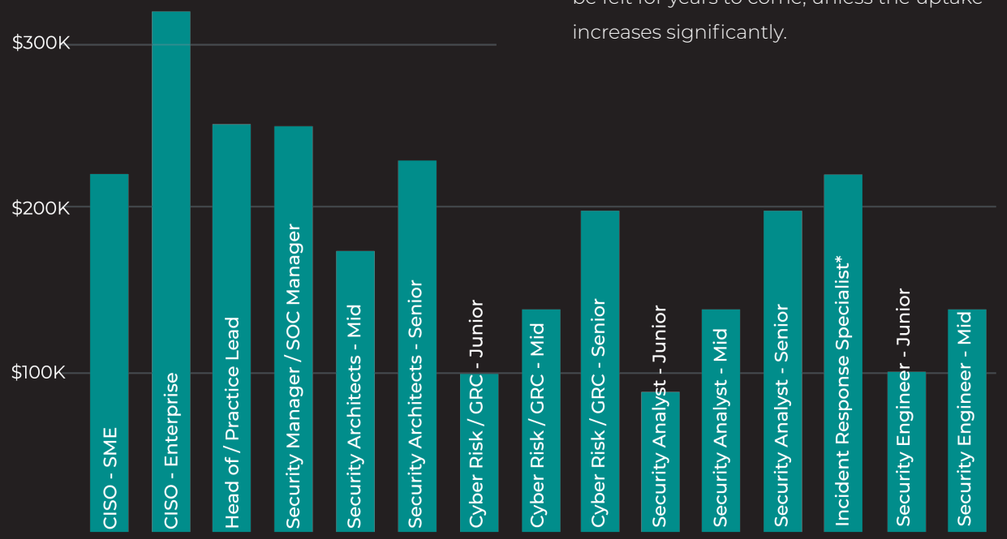
Across the board in 2020/21, we've seen an increase in salaries for the cyber-security sector. In addition, some specialist skillsets that are more highly-sought-after, are seeing even larger increases. The primary areas where we have seen the largest demand are security operations, GRC and specialist areas such as incident response and threat hunting.

Across some locations, the cyber security recruitment market experienced a pause in the last 6 months of 2020. Melbourne was the worst impacted city, with Brisbane and Canberra remaining relatively unaffected Understandably, candidates were concerned about making a move in this time, and many organisations delayed hiring decisions. The market picked up again in early 2021 and is currently very buoyant with most organisations recruiting or intending to recruit.

"2021 has seen the pent up demand for cyber security resources causing a spike in demand like we have not seen since Y2K."

This increase in demand and confidence has seen people once again considering new opportunities. Despite the slowdown in 2020, the workload for cyber security professionals did not subside. In fact, it increased - due to the large-scale digitisation that businesses experienced. This was largely because of an increase in work-from-home-policies, a surge in cyber attacks and a widening threat across digital landscape.

Graduate and entry level recruitment effectively stopped during 2020 due to COVID-19 which gave us 12 months of minimal graduate or entry level intake. The impact of this talent vacuum will likely be felt for years to come, unless the uptake increases significantly.



Migration

Whilst ICT Security professionals hadn't been defined as a critical skill for travel exceptions, in 2020 they were regularly approved. 2021 has seen the pent up demand for cyber security resources causing a spike in demand, the likes of which we haven't seen since Y2K. Surprisingly this year the listed critical sectors of employment are being more strictly applied, therefore making it harder to receive exemption for cyber security professionals to migrate to Australia. This has further exacerbated the talent shortage issue and led to an increase in salaries.

Remote work & flexibility

We have seen notable increases in remote work and work from home arrangements. However many organisations still have a preference for staff to be on-site at least once a week.

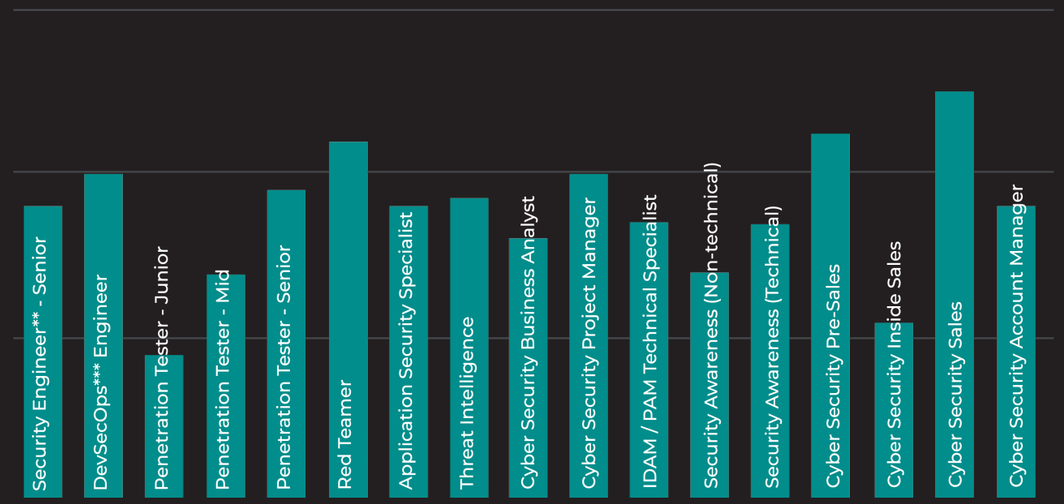
Contract & temporary workers

We have seen very little change in the number of contract workers despite the increase in demand. Canberra still has a disproportionately high number of contract workers, followed by Sydney and Melbourne. We anticipate an increase in demand as the market continues to tighten, however there remains a strong preference for permanent staff across most of Australia.

Training & development

We have seen an increase in the provision of training for employees with many organisations offering a fixed AUD amount as part of their salary packages.

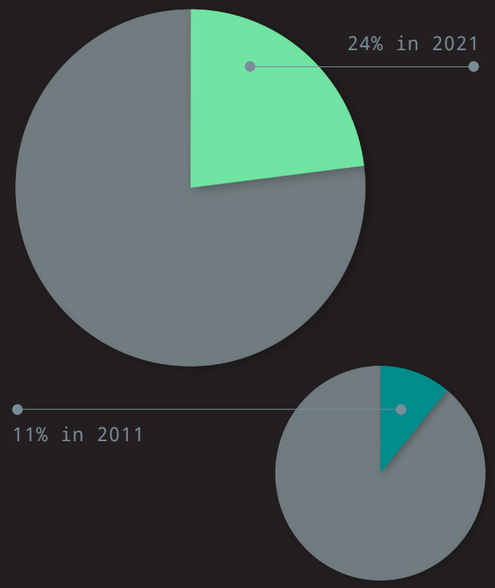
Global vendors are winning the war for talent by outbidding local organisations with their lucrative packages. These often include significant benefits such as RSU's and health insurance.



Analysis

Diversity

According to a ISC2 global workforce report, out earlier this year, 24% of the cyber workforce is now female (up from 11% in 2011). Whether this stat is truly reflective of the Australian market is unclear. There are more female cyber security students coming through the new cohorts, however in spite of a more diverse candidature across GRC and Security Awareness - there still remains a lack of diversity in technical areas such as Penetration Testing and Security Operations. More employers are pushing for diversity, but sadly many are still not creating specific plans or pipelining to create diverse teams. The desire to hire more females in Cyber has meant salaries for new hires are increasingly moving towards being on par with their male counterparts. However we still have a long way to go to increase female participation in the industry.



Percentage of women in the cyber workforce.

CISO's

We continue to see the emergence of new CISO roles in SME's and the elevation of the role from a technical role to a true executive position. Interestingly, some large ASX listed organisations are yet to appoint a CISO.

80% of APAC organisations are reported to have suffered a cyber attack in 2020 (SecurityBrief NZ)

Governance, risk & compliance (GRC)

Increased media coverage of cyber attacks is driving action from executive teams and boards wanting a more holistic approach to GRC. The rise in personal liability of boards and executives overseas, has increased the level of concern locally. Third party risk requirements and demand in ISO27001 certification are prevalent in the market. The rise of more strategically focused cyber security roles, advising boards and consulting on large digital transformation projects - will drive demand for these roles further.

Security Operations

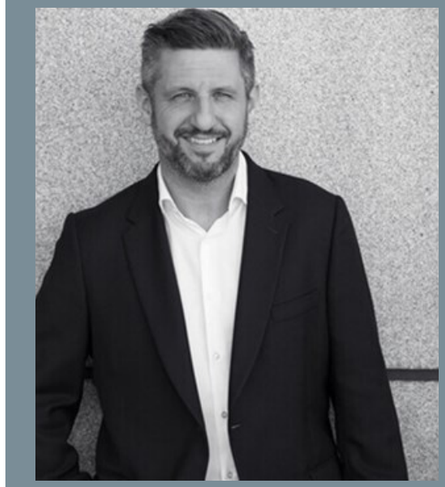
Security Operation Centres (SOC) continue to increase in size, scope and complexity. As a result we are seeing more defined roles and higher level skill sets required across several roles. These are mainly for SOC analysts, engineers, incident response and threat hunting. The demand for SOAR, Artificial Intelligence and Machine Learning security experience is ever increasing.

Offensive Security

Penetration testers remain in demand. The CORIE framework has resulted in large enterprise and service providers building or growing their red team capability.

OT Security

In 2020, the Australian government passed an amendment to the Critical Infrastructure bill, increasing its coverage and requirements. A report by PWC states that over half of the cyber executives they surveyed said that sponsored attacks on critical infrastructure are likely. This is cause for concern for many critical infrastructure environments due to legacy operational tech systems (OT) - such as Industrial Control Systems (ICS), becoming closely integrated to IT systems. This in turn makes them highly attractive targets for cyber attackers looking for insecure entry points. Overall, cyber OT roles are becoming more commonplace and we predict that this will only continue to grow over the coming years.



"On a more personal level the past year has been tough due to Covid. However the Cyber Security industry is now busier than ever, and it's been great to help new companies start up and existing teams to bolster their cyber number. I'm hoping we will soon be able to attend domestic conferences and meetups so we can get together as an industry, swap ideas and raise a glass to each other for continuing to thrive throughout these challenging times."

Matt Dunham
MANAGING DIRECTOR

In summary

2021 is now an exciting and buoyant market for job-seekers and a challenging market for employers. The increasing maturity in the Australian Cyber Security sector, coupled with near zero migration has further intensified this predicament. We will likely see a continued fight for talent and a further increase in salaries until the challenge of migration is addressed and the training and development of local talent is developed to meet the ever increasing requirements.

Our recommendation would be for employers to pipeline for talent and ensure their candidate experience is high-end. In addition they should ensure that their recruitment processes are streamlined - in order to attract, engage and secure the best talent in the market.

"2021 has accelerated an employment market that we all knew was coming. Increased attacks and tighter regulation, with the added effect of border closures - has created a hot market for jobseekers and a challenging one for employers."

Paul Jenkins
DIRECTOR

"44% of respondents to a 2020 digital census indicated "their ability to access the skills they need to innovate and grow" was one of their top 3 challenges. (AusCyber 2020)"

Decipher Bureau

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, the Middle East and SE 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 & 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