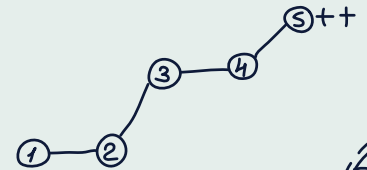
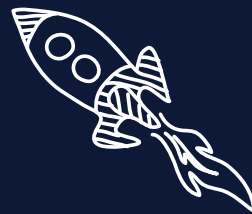




Cyber Wrap **FY 2022-23**

Prepared July 2023

Sydney | Melbourne | Brisbane



What is the Cyber Wrap?



Hey there, we're glad you've found us.

Do we have a treat for you.

Meticulously crafted from a wealth of data sourced from LinkedIn, our extensive experience in diverse roles, and invaluable insights directly shared by candidates – the Talenza Cyber Wrap is your golden ticket to unraveling the world of Cyber talent in 2023/2024

Now, let's address your burning most asked questions:

"What's the buzz in the market?"

"What do candidates seek in today's landscape?"

Rest assured, we're here to provide the answers. Through insightful conversations with our clients and diligent trend analysis, we've distilled the essence of the market for you.

Capturing a holistic view of the market is no easy feat. Fortunately, our privileged position at the forefront of the industry equips us with the ability to uncover invaluable insights. And now, we're thrilled to share this wealth of knowledge with you through this comprehensive report.

Our ultimate mission? Facilitating seamless connections between exceptional talent and the perfect roles. With this guide, we're ready to tackle your toughest hiring challenges head-on and keep you well-informed in this ever-evolving landscape. Trust us to navigate the dynamic twists and turns, empowering you to make informed decisions with confidence.

What's in this guide for you?



HR / P&C

- *Present an attractive offer to technology and project services talent to attract and retain them*
- *Engaging the hearts and minds of talent is the most sustainable source of competitive advantage. But first, you need to know what they want.*
- *Align your EVP with real market evidence to attract and retain top talent*
- *Keep up with industry demands and changing motivations of technology and project services talent*
- *Create experience that employees want to talk about (promoting advocacy)*

Hiring Managers

- *Educate your talent team on the nuances of technology and project services talents motivators*
- *Keep up with industry demands and changing motivations of technology and project services talent*
- *Get top talent who are motivated and engaged to deliver on your projects*

Talent Acquisition

- *Better negotiate with candidates that have multiple offers*
- *Position your offer based on key candidate drivers rather than just salary*
- *Adopt a human-centric way of thinking in recruitment and talent acquisition*

Executive Summary



Meticulously crafted from a wealth of data sourced from LinkedIn, our extensive experience in diverse roles, and invaluable insights directly shared by candidates – the Talenza Cyber Wrap is your golden ticket to unraveling the world of Cyber talent in 2023/2024.

At Talenza, we understand the importance of accurate budgeting, and that's why we proudly present our observed salary guide. This invaluable resource serves as your compass, providing insights into industry standards. While outliers exist, our data is representative of approximately 90% of the market, ensuring you make informed financial decisions.

Financial year 2022-2023 was a tale of two halves. We saw incredibly fast acceleration of salaries in the first half with multiple factors driving this.

Low interest rates, growing team sizes internally and in consultancies – this combined with low migration rates for 2-3 years meant the shortage for talent at mid and senior levels worsened.

In the latter part of the fiscal year, significant redundancies rocked the landscape, particularly within esteemed tech giants like Atlassian, AWS, Avanade, Microsoft, and notable cyber players like CrowdStrike, NCC Group, and Trustwave. This sudden wave of workforce changes resulted in an influx of candidates flooding the market, leading to a stabilization of salaries.

Moreover, data breaches emerged as a prominent concern during this fiscal year, with notable incidents involving Optus, Medibank, Latitude Financial Services, and more. The repercussions were far-reaching, triggering legislative modifications. Changes to the Australian Privacy Policy, SOCI, and APRA CPS230/234 began to fuel demand for roles related to Governance, Risk, and Compliance (GRC).

As the market adapts to these shifts, it's vital to stay attuned to

Contents



01. Intro to Talenza Cyber

02. Cyber Predictions

03. Supply Market Insights

04. Market Drivers

05. Attracting diverse talent

06. Defensive Talent Insights

07. Application & Product Security Insights

05. Offensive Security Insights

06. GRC & Architecture Insights

07. Leadership Insights

08. Getting started in Security

09. About us

About Us

We are fortunate to have three experienced and well-respected consultants working together to assist our clients looking to attract the best talent.

Chelsey Costello



Heads up our cyber team in Brisbane, she is a cyber talent sniper with a track record of delivering and a leader for diversity in information security. Chelsey has been appointed the Brisbane Chapter Lead for AWSN and was nominated for the 2021 AWSN Unsung Hero Award.

Riki Blok



Heads up our cyber operation in Sydney, since joining Talenza. Riki is a long serving industry advocate and only operates with honesty, integrity and hard work. His long-standing clients and candidates are testament to his ability to build and keep relationships.

Brittany Buswell



Joining Riki in Sydney, Brittany brings an exceptional track record in sourcing top-tier Cyber experts across Australia. Paving her way through building trusting relationships and consciously understanding her clients pain points.

Talenza **Cyber** Predictions for the next 12 months



Compliance Changes

- High profile breaches and natural maturing are driving compliance changes.
- The update to the Australian Privacy Act, APRA CPS230, SOCI act are driving an uplift in general to industry.
- We are seeing this drive demand for GRC resources. We expect to see the Technical roles to follow in the latter half of the financial year



100% remote work is on the way out

- What was the norm for a couple of years in response to Covid-19 lockdowns is on it's way out.
- Being paid over market salary for a fully remote role will become the exception rather than the rule.
- We are seeing enterprise customers pushing for multiple days in the office and we beginning to see this having a flow down to most companies



Salary Changes

- We saw incredible acceleration of salaries over the last financial year.
- This year we believe there will be a balancing of salaries due to a combination of factors including rising interest rates, redundancies and shrinking of global economies.
- They won't go down necessarily, but 20-30% jumps will be harder to secure.

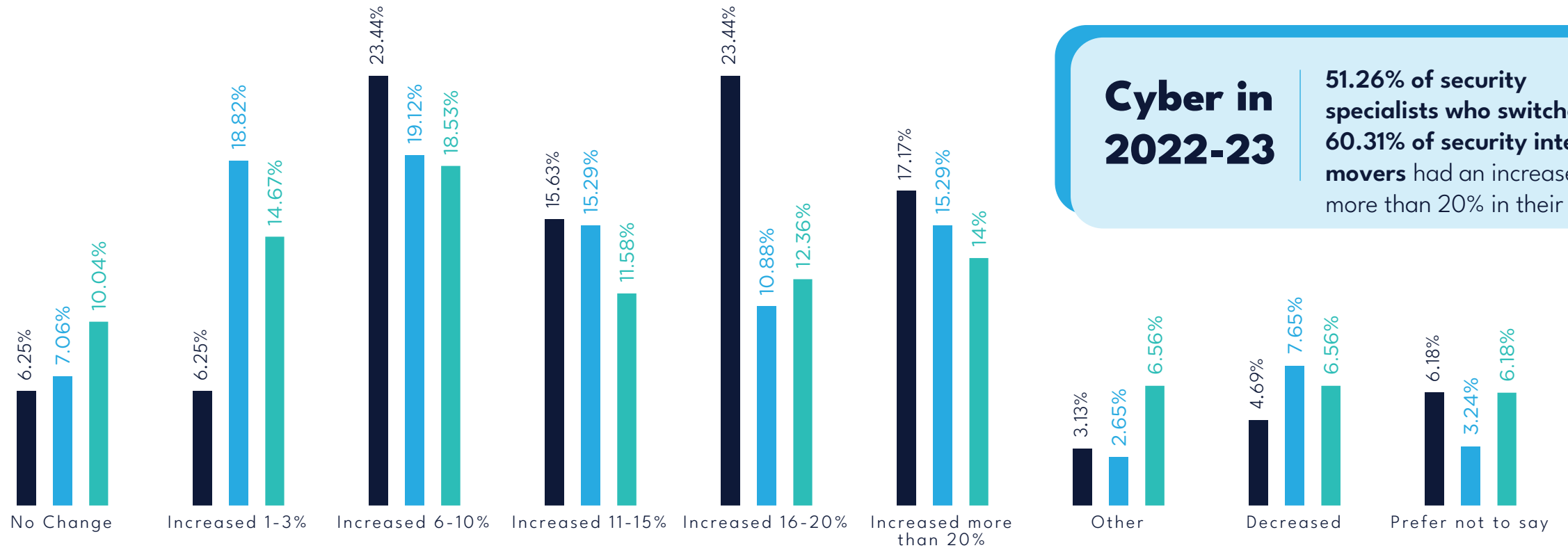


Employers market

- For the majority of the last 18-24 months it has been an employees market.
- This meant less experienced candidates who were a moderate match were sometimes receiving 2-3 offers within 1-2 weeks of making themselves available on the market.
- Role availability will become less and the balance will shift back towards the employers

Movement and Salaries across Technology in 2022-2023

■ Internal Move ■ Salary Change Switchers ■ Salary Change Stayers



Cyber in 2022-23

51.26% of security specialists who switched and 60.31% of security internal movers had an increase of more than 20% in their salary.

Disclaimer: The data provided in this guide is sourced from information gained by Talenza over the past 12 months recruiting 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. 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. Talenza do not hold any liability for the accuracy of this information.

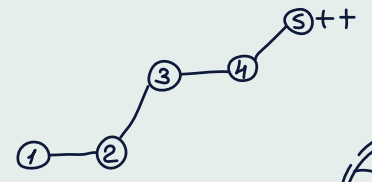
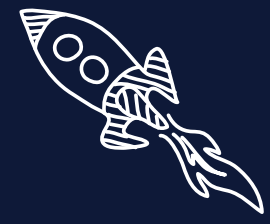
Our interpretation of ~~salaries~~





Supply Market Insights

Sydney | Melbourne | Brisbane



Intro – market insights



Where is it from, why is it important and what can you use this for?

Median tenure slightly increased as did overall industry headcount.

24,922

Professionals

1,500

Industry wide
headcount growth



1.4 years

Median Tenure

20% female

Gender split

Cyber Security Market Supply

18%

of the workforce has changed
jobs in the last 12 months.

What education do they have?

- TAFE NSW
- Charles Sturt University
- RMIT University
- UNSW
- Monash University

The supply of emerging specialists



32%

(almost 1 in 3) of the workforce has changed jobs in the last 12 months.

What education do they have?

- Deakin University
- UNSW
- RMIT University
- Monash University
- Charles Sturt University

0-5 years of experience

2,823

Professionals

909

Changed Jobs

0.8 years

Median tenure

Gender split

27% female 73% male

5-10 years of experience

3,499

Professionals

820

Changed Jobs

1.3 years

Median tenure

Gender split

25% female
75% male

The supply of mid level specialists



23%

(almost 1 in 4) of the workforce has changed jobs in the last 12 months.

What **education** do they have?

- TAFE NSW
- Deakin University
- University of Technology Sydney
- UNSW
- Charles Sturt University

The supply of **senior** specialists



16%

of the workforce has changed jobs in the last 12 months.

What **education** do they have?

- TAFE NSW
- RMIT University
- Swinburne University of Technology
- Charles Sturt University
- UNSW

10-15 years of experience

3,428

Professionals

548

Changed Jobs

1.8 years

Median tenure

Gender split

20% female 80% male

15- 30 years of experience

6,614

Professionals

840

Changed Jobs

2.1 years

Median tenure

Gender split

16% female
84% male

The supply of experienced/ executive talent

16%

of the workforce has changed jobs in the last 12 months.

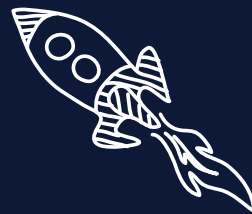
- **What education do they have?**
- TAFE NSW
- RMIT University
- Swinburne University of Technology
- Charles Sturt University
- UNSW



Market Drivers

Bespoke research from Talenza

Sydney | Melbourne | Brisbane



Intro – market drivers



Where is it from, why is it important and what can you use this for?

EVP etc

Cyber Candidate Motivator Highlights



37%

Of cyber professionals utilised their training budget over the past 12 months. 23% said they aren't offered one.

Maintaining work life balance is the biggest concern for Cyber professionals in the next 12 months.



54%

of all respondents said they plan to change jobs in the next 12 months. Of those people, 36% of them changed jobs in the past 12 months.

#1

driver for female respondents is

Tied between flexible working arrangements + providing an attractive salary with getting a promotion the biggest concern for women next year.



76%

of respondents say that providing an attractive salary and benefits is in the top 5 most important factors when considering a new employer.



56%

of respondents indicated a **poor relationship** with their managers or colleagues motivated them to change roles with a new employer.

Non-monetary benefits



are important to 95% of cyber professionals considering a new job.

Training and development

has dropped since last year from #2 spot to #9. 34% of people still say it's important to them.

Executives say their biggest concern

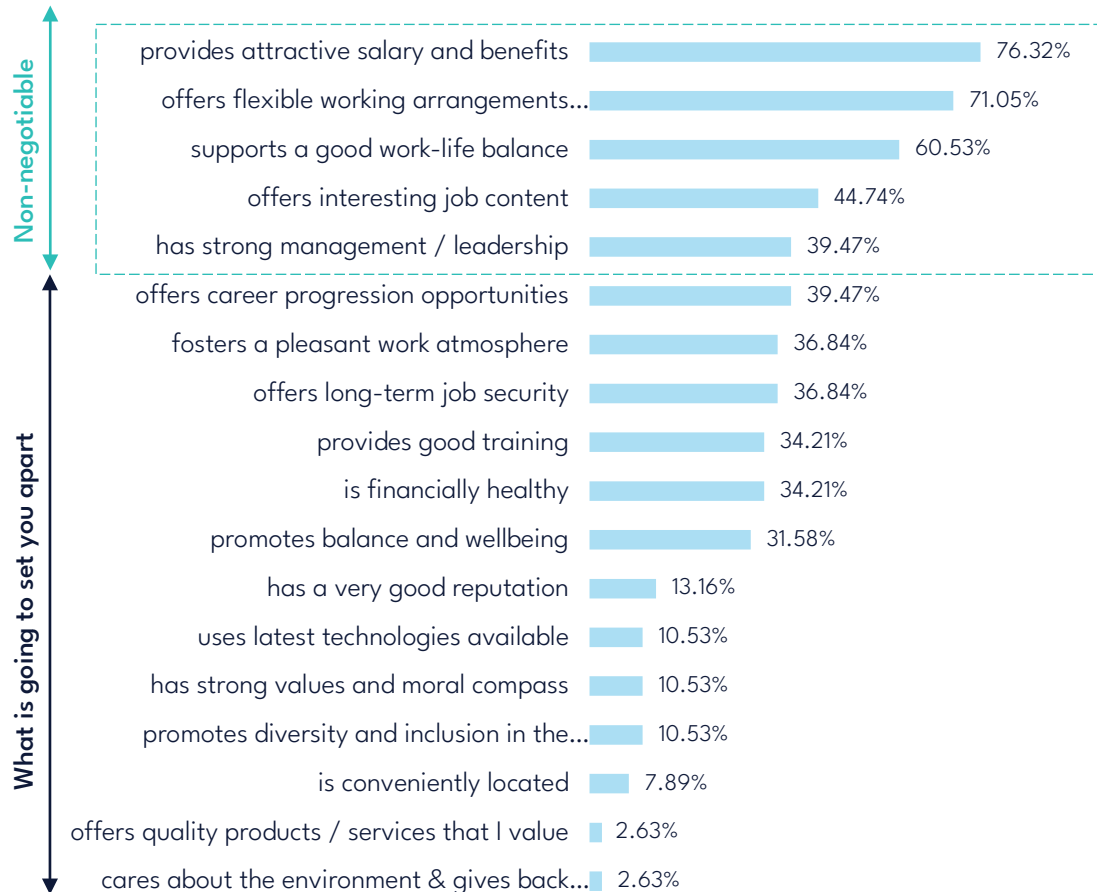
over the next 12 months is boosting their salary.

Top Drivers for Cyber Talent 2023

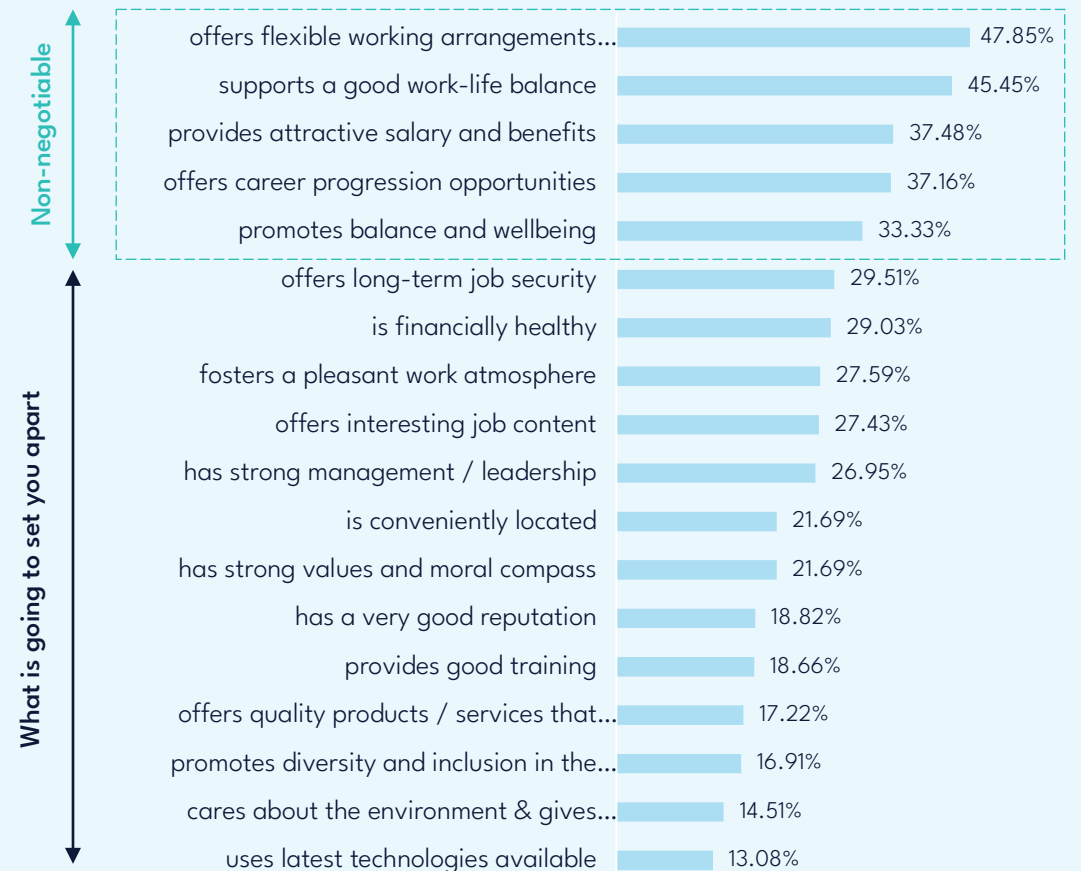


Top Drivers Cyber vs IT 2023

Cyber top drivers



IT top drivers



Top Drivers Cyber 2022 vs 2023

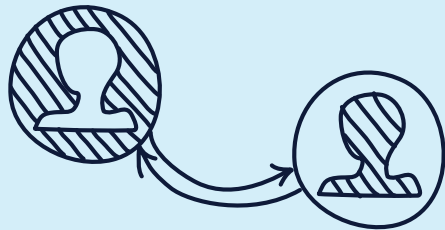
Cyber top drivers 2023



Cyber top drivers 2022



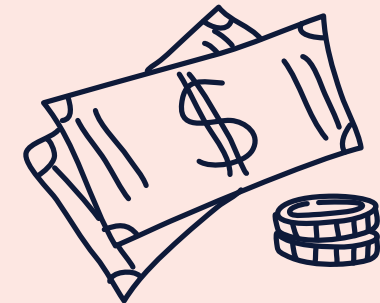
Re-defining the **Cyber EVP**



Strong management and relationship with direct manager is a huge driver now up to #5.



Training is showing as less important this FY, however almost all candidates mention it as important.



Salary is the biggest driver – we suggest this is driven by interest rate pressures and the continued scarcity of cyber talent.

Using these insights to ~~redevelop~~ your EVP



- **Job family specific content**
- **Examples of what this can look like in action**
- **Link to candidate motivator report**
- **[Read this article](#)**



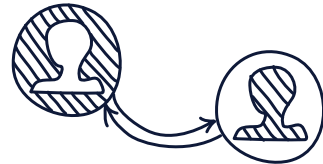
Attracting diverse talent

Sydney | Melbourne | Brisbane



Attracting diverse talent

At Talenza Cyber, we are fortunate to have Australia's two leading female, cyber security recruitment consultants.



Both are deep advocates for inclusion, diversity and equal employment opportunities. Their involvement with the Australian Women in Security Network gives them direct access to emerging female talent networks.

They are well positioned to provide advice, guidance and insights on how to improve your EVP to attract candidates from diverse backgrounds.

As the data we have sourced from LinkedIn shows, females are still very underrepresented in cyber at 20% overall. This drops to 16% for executive level roles, however we are beginning to see this shift in industry. For early career candidates with 0-5 years of experience, this is 27% overall.

We have noticed with our clients that now more than ever, attracting and retaining a diverse team is more of a focus. The information that follows should be used to inform and give some guidance on how to attract and retain a diverse workforce.

Attracting Women



Based on what we have seen over the last 12-24 months, here are some strategies you can use to ensure you attract a more gender diverse talent pool.



Use gender neutral language with less requirements

- Females are less likely to apply unless they hit 9/10 requirements
- Tools like [this](#) one can amend your adverts to use gender inclusive language to attract more females



Include women on interview panel

- Show an inclusive and diverse team on interview panels
- This improves candidate experience and gender bias
- We have had females withdraw from roles due to lack of female representations




Ask deeper questioning and reassurance

- Females are more likely to downplay their achievements and therefore deeper questioning is often required to draw this out
- It might be as easy as asking for further examples on project deliverables and specifics around their contributions



Help champion females in cyber

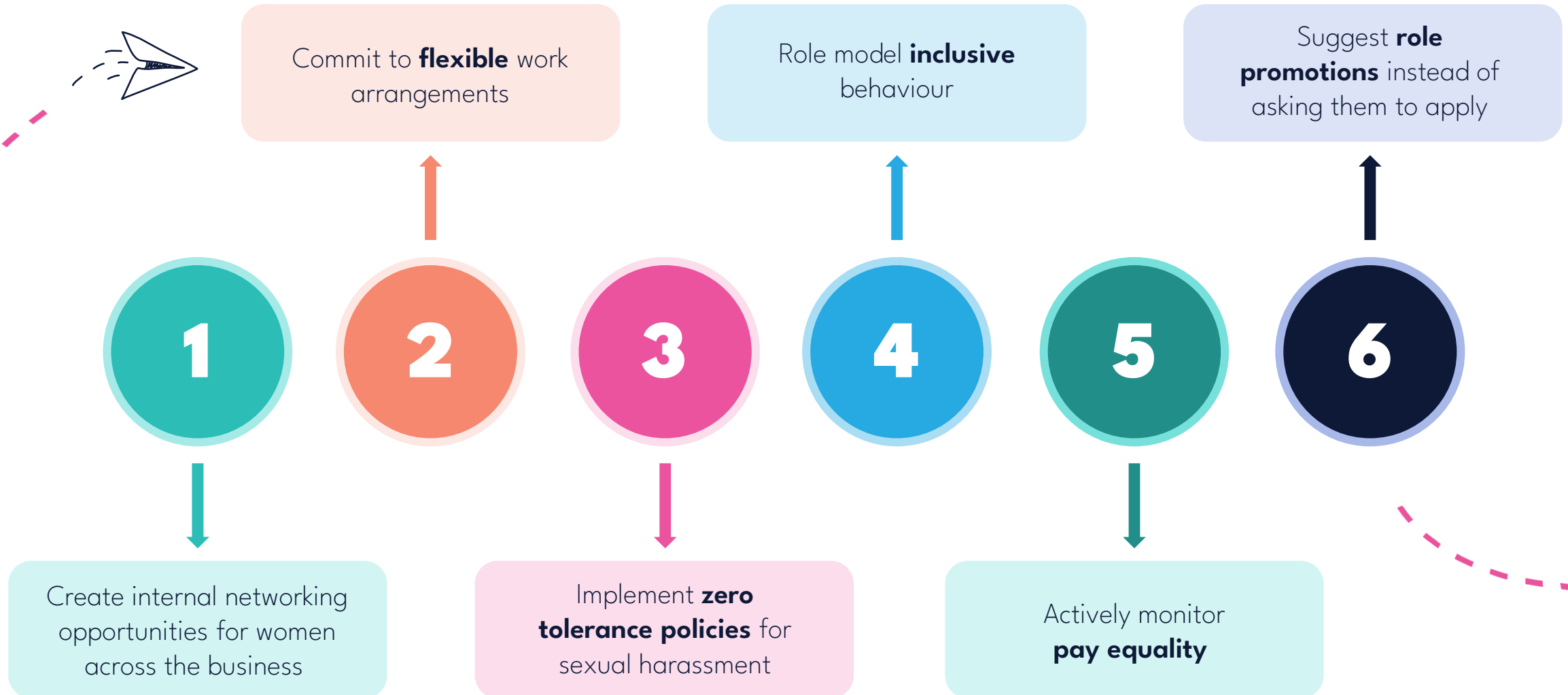
- Invest in and support initiatives to increase females in cyber
- The Australian Women in Security Network (AWSN) is a great example of this
- This highlights your commitment to diversity and is an attraction



Of the **27%** that join the technology industry, more than **50%** are likely to quit before the age of 35, and **56%** are likely to quit by midcareer.

Retaining Women ...

Once you have found women from your organisation, it's important to retain them:



Case Study: Pay Transparency

Pay transparency should be used as an enabler to address the gender pay gap. This is not always the case unfortunately and is sometimes used to in negative ways.

Scope

- A female who was very underpaid in her current role by approximately 30%.
- She had stayed loyal to her current company and had been given raises in line with CPI rather than market increases for her skillset.

Challenges

- There was a male and female going for this role, with an offer made to both.
- The offer for the male candidate who was less qualified and experienced was 20% higher.

Outcome

- Our team addressed this gender bias and had the offer amended to reflect their market worth rather than a % increase on existing package

EVP Drivers for Females in Tech

57% of women

Who changed jobs in the last 12 months noted that a poor relationship with a manager or colleague was a driving factor.

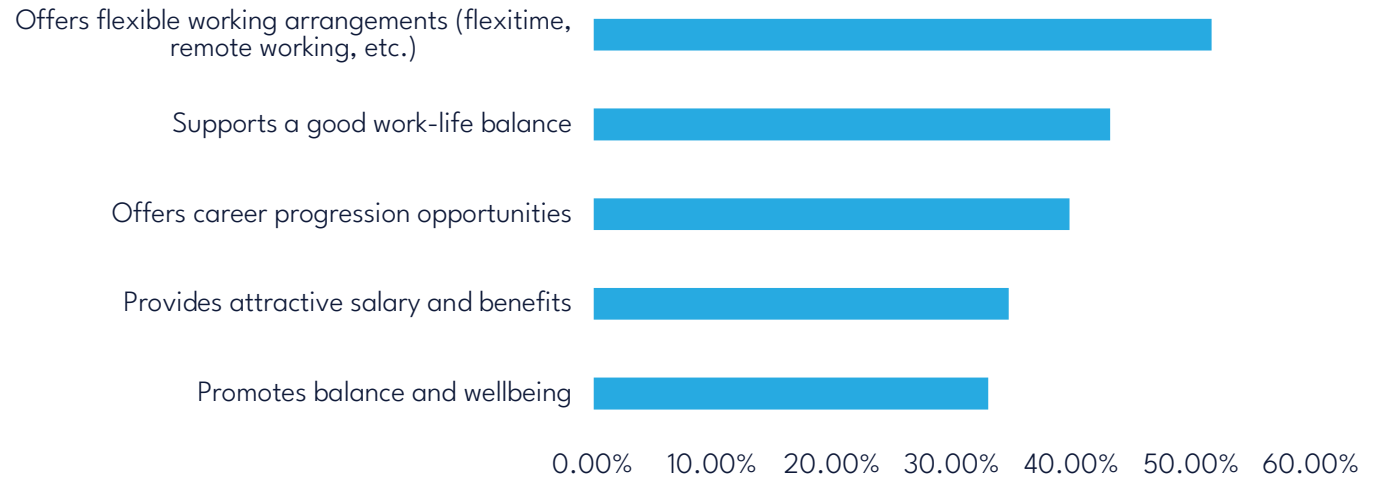
1 in 3 of women

who changed roles in the same organisations saw a salary increase of over 16% in 2023.

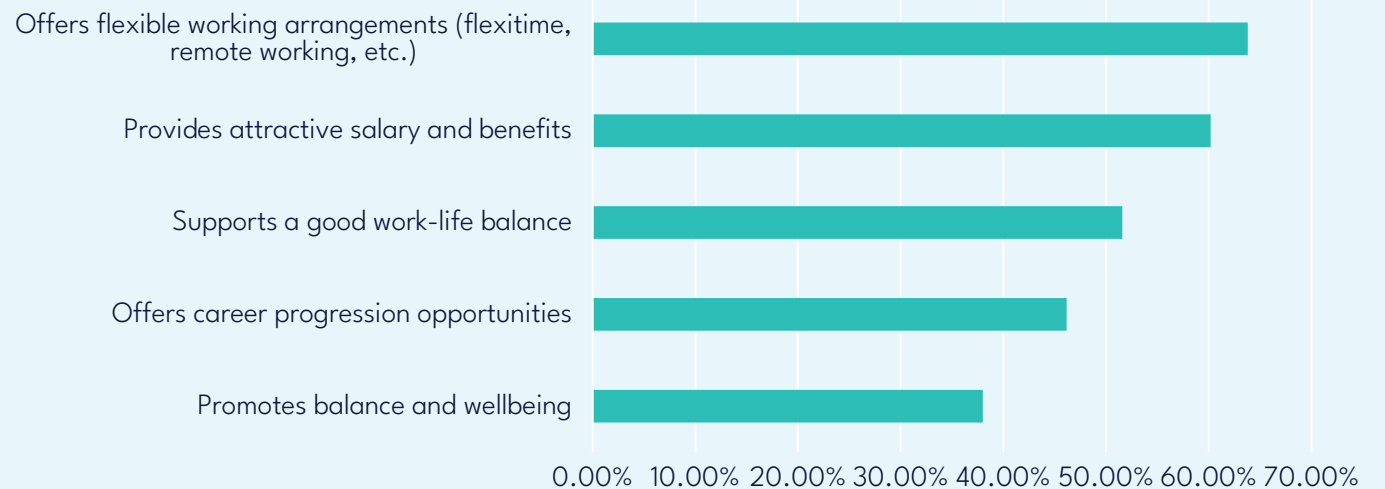
For males who got a new job with the same organisation, 46% saw an increase of over 16% in salary.

Top EVP Drivers Female Talent 2022 vs 2023

2023



2022





Defensive Talent Insights

Sydney | Melbourne | Brisbane



Defensive security

We have seen a huge uplift in cyber defence roles – there was a 12% growth overall and 29% growth in 0-5 year experience headcount.

Incident Response and Cyber Threat Intelligence capabilities were bolstered in house and in consultancies in response to the changes to APRA CPS230 and SOCI act.

The roles we saw the highest volumes of over the last FY were in Security Engineering and Security Analyst / Incident Response / DFIR style roles.

Salaries for junior and mid level accelerated significantly as a result, we saw top end salaries for technical resources eclipse the \$200k mark which was unheard of outside big tech companies a few years back.



Key insight

Interactive acquired Slipstream, we believe we will see them take on traditional players like IBM, Secureworks, Mandiant and CrowdStrike.

Breach preparedness and post breach response has been a big focus – likely driven by the high profile breaches and compliance uplift.

Multiple law firms are building an offering or upping their capability, this is creating an additional option for candidates and further shortening candidate supply.

We predict Azure Sentinel and Defender365 to be the hottest technologies in Defensive Security.

Automation is continuing to be built out in most security teams also.



Summary of **talent** in this space

1.3 years

Median Tenure

Diversity

21% Female

79% Male

Most in demand
cyber area

**12% headcount
growth**

Talent source

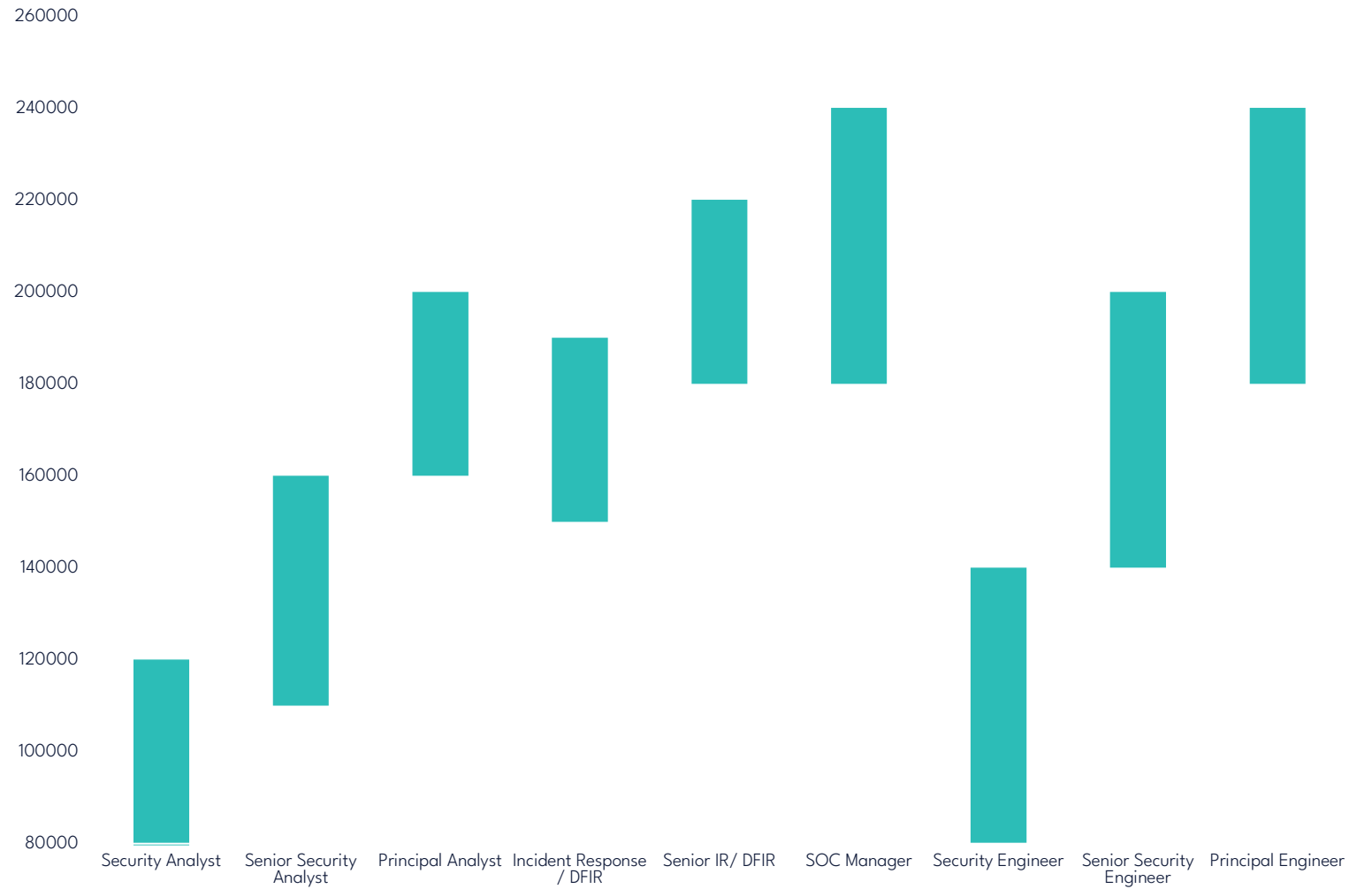
- TAFE NSW
- Charles Sturt
- Edith Cowan
- RMIT University

Defensive Security Base Salary Range



The green boxes represent the base salary range for each role.

For example our observed Security Analyst base salary sits between \$80K - \$120K.



Disclaimer: The data provided in this guide is sourced from information gained by Talenza over the past 12 months recruiting 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. 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. Talenza do not hold any liability for the accuracy of this information.

Case Study: SOC roles



Challenge

- Global Consultancy business who were expanding capability in Splunk and adding in Sentinel capabilities.
- Due to the customer facing criticality of these roles, a high level of technical skill and communication skills were required.
- These roles had already been open for several months under internal and agency management.

Approach

- For these remote first roles, we mobilized our teams in Sydney and Brisbane for this search.
- We approached passive and active candidate pools, we needed strong technical and consulting skills.
- To assess this we had a questionnaire and met all candidates in person or by video.

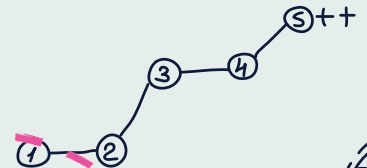
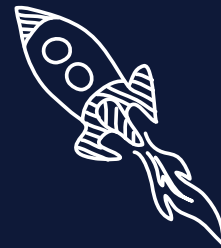
Outcome

- There was a higher demand for the Splunk Engineers, we delivered 2 placements within 3 weeks.
- This alleviated the concern of losing critical clients and projects that were in process.
- In total our team placed a total of 7 placed into their teams across Azure Sentinel engineering, Splunk engineers and SOC analysts within a 4 month period.

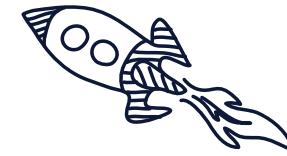


Application & Product Security Insights

Sydney | Melbourne | Brisbane



Application & Product Security



We have noticed a maturing of this space is ongoing, internal Application Security and Product Security teams are growing on the whole.

Big Tech companies like Canva and Atlassian team sizes generally grew though redundancies at Atlassian at the start of 2023 did affect this slightly.

The traditional leader for AppSec consulting work was Ampion/Shelde/Wipro, however bespoke consultancies are beginning to pop up in this space, with smaller, specialised AppSec focused consultancies like Galah Cyber.

We are also noticing a trend for Offensive Security Consultancies to begin offering this as a service too with The Missing Link and CyberCX amongst others growing offerings in this space.

We expect this to be a high growth sector over the next 12-24 months as internal teams are built at more companies. The Optus breach in particular being an example where basic Application Security hygiene could have prevented an incident.



Summary of **talent** in this space

1.4 years

Average Tenure

Diversity

15% Female

85% Male

Tech Companies are
the biggest employers

Atlassian

Canva

MYOB

Talent source

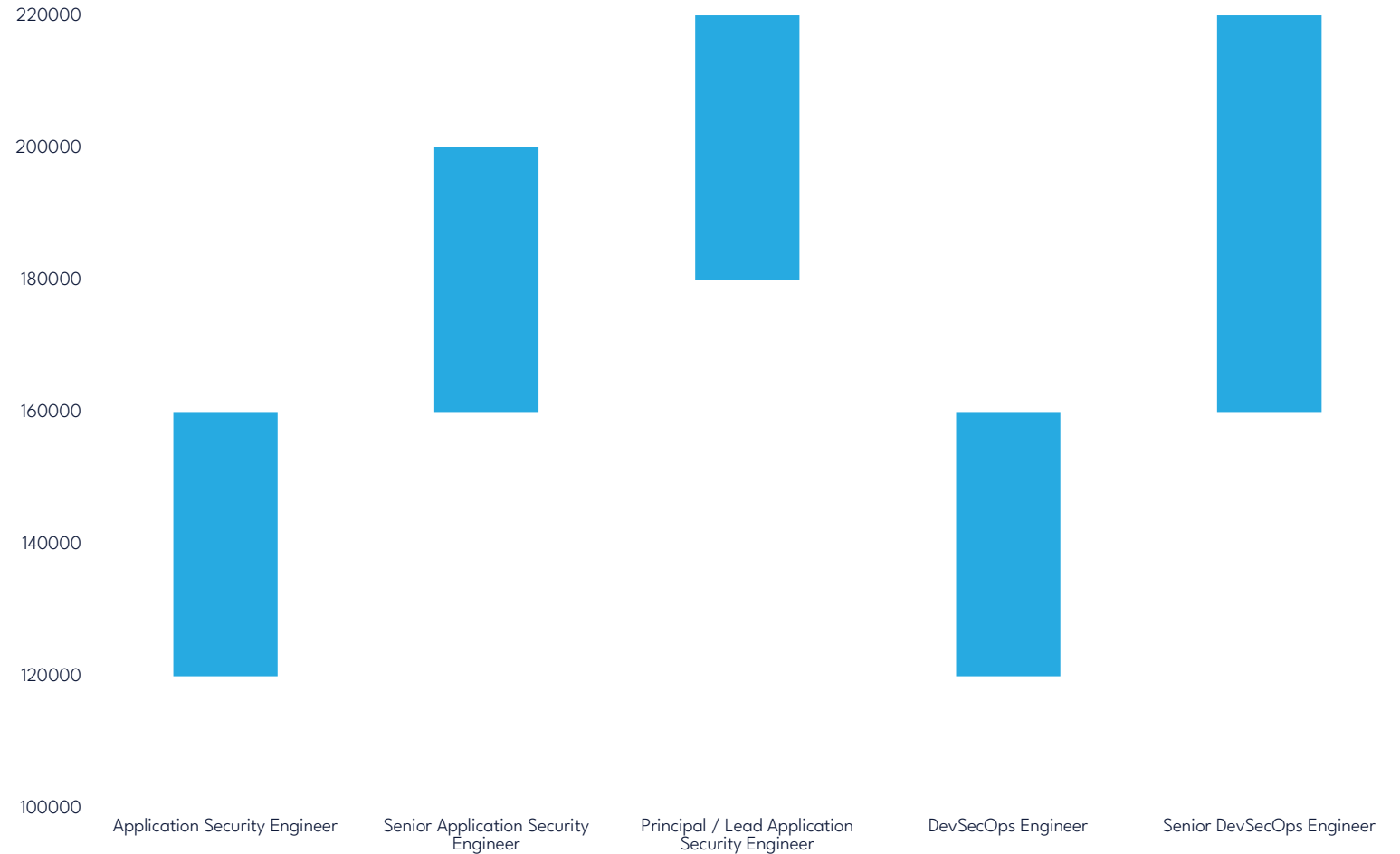
- UNSW
- Deakin
- RMIT
- Monash

Application & Product Base Salary Range



The blue boxes represent the base salary range for each role.

For example, our observed Application Security Engineer base salary sits between \$120K - \$160K.



Disclaimer: The data provided in this guide is sourced from information gained by Talenza over the past 12 months recruiting 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. 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. Talenza do not hold any liability for the accuracy of this information.



Case Study: Product Security

Challenge

- A global media organization was building a Product Security Team in Australia.
- The Lead role had been open for a number of months before Talenza Cyber was engaged.
- We were briefed on the role and unique challenges it possessed by the global team in the US.

Approach

- There was a preference for East Coast candidates, our search was targeted on Sydney and Melbourne.
- Due to a requirement for technical and leadership skills, video interviews along with technical screening used to assess this.

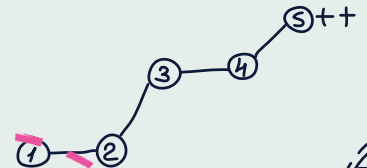
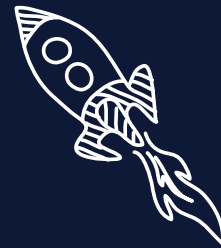
Outcome

- We located the lead from a large financial services team, that person moved across at the same salary as they were currently on.
- Following on from that successful placement, we built their team around them.



Offensive Security Insights

Sydney | Melbourne | Brisbane



Offensive Security insights



Internal Offensive Security and Red Team offerings have been steadily growing, we noticed a number of senior testers move from consultancy into internal teams within financial services. CBA, Westpac and NAB are a few companies we have seen bolstering their internal functions over the last financial year.

Big tech has also been growing their internal functions, providing further pressure on an already small talent pool.

Key Mergers have slowed this year in Australia, CyberCX, and Sekuro all seem to have stabilised as an aim over the last financial year. Big 4 consultancies have generally grown their team sizes again, PwC and Deloitte appear to be rebounding the quickest.

A lot of niche players have popped up creating additional competition for an already small candidate pool.

We have seen a huge uplift in the salaries of junior and mid level testers over the last 24 months. The time for a pen tester to reach a salary of \$130k + super is often around the 3 years experience mark. This salary was previously a 5+ year tester.

Salaries generally top out at the \$150k - \$180k + super sort of range for individual contributor roles in consultancies. We do see some reach to \$200k + super but these are rarer.

Above this range, you will be expected to work on management or a technical lead role.



Summary of **talent** in this space

1.8 years

Average Tenure

Diversity

11% Female

89% Male

Consultancies are the
biggest employers

CyberCX

EY

CBA

1 in 4

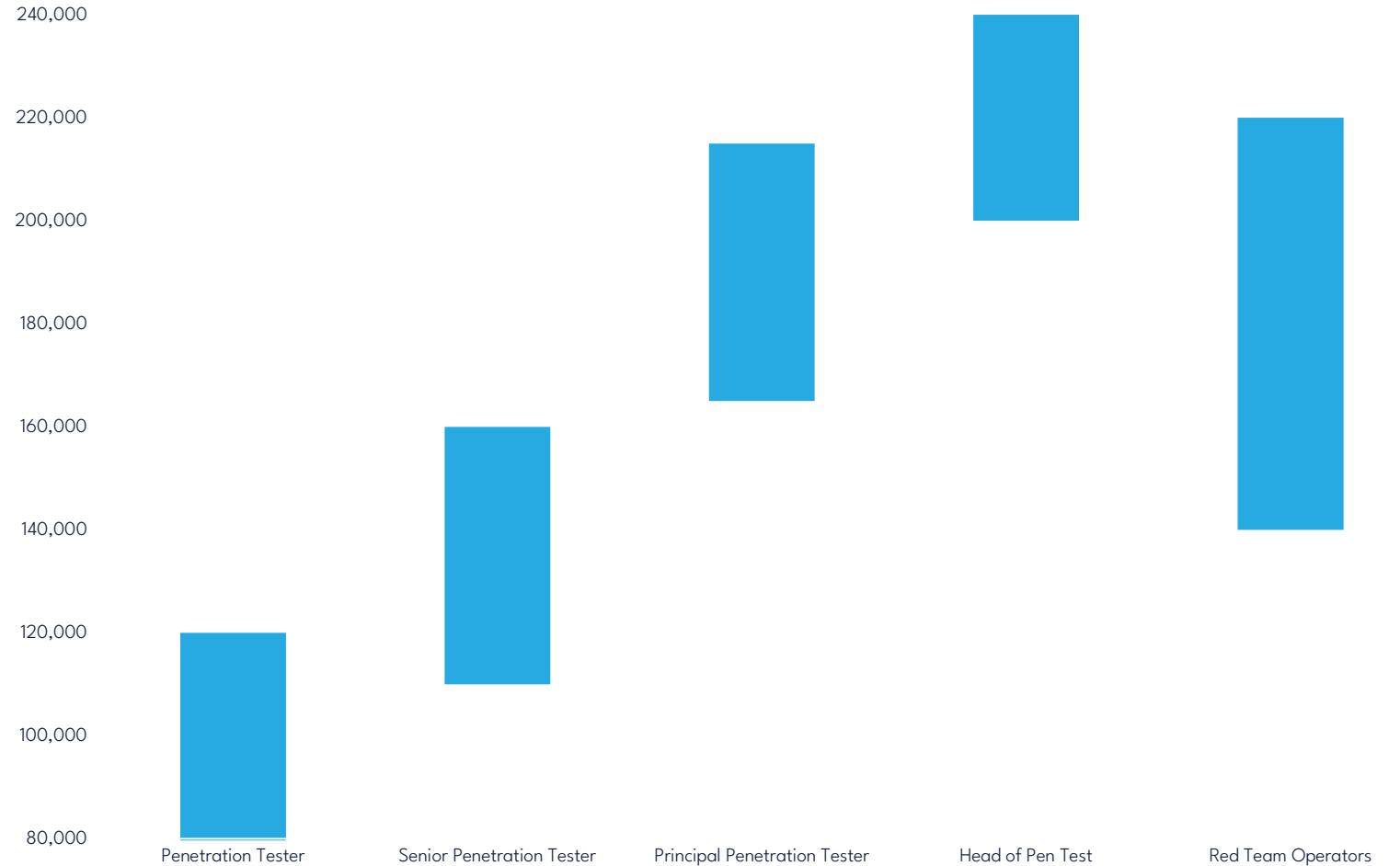
changed roles

Offensive Security Base Salary Range



The blue boxes represent the base salary range for each role.

For example, our observed Penetration Tester base salary sits between \$80K - \$120K.



Disclaimer: The data provided in this guide is sourced from information gained by Talenza over the past 12 months recruiting 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. 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. Talenza do not hold any liability for the accuracy of this information.

Case Study: Offensive Security



Challenge

- A Specialised Security Consultancy with around 25 pen testers was growing due to new clients.
- A very high level of technical capability in their teams, had exhausted local talent pools so they decided to engage Talenza Cyber.
- Minimum requirement of OSCP certification and 5 years experience identified

Approach

- Custom searches for industry involvement, certification and known consulting businesses
- We developed 6 questions to screen candidates on calls, followed up with video
- As sponsorship was available, we assessed written English by email response to questionnaires

Outcome

- Initial shortlist of 3 candidates presented within 10 days, all candidates were video interviewed prior to submission.
- 2 of the 3 candidates were interviewed, with the preferred candidate identified and offered the role along with a sponsored visa.



Case Study: Offensive Security

Challenge

- A well established boutique Security Consultancy with 5 testers and over 10 years experience providing service engaged us for a xxx role.
- This company had not had success using an agency previously and had been looking for 3 months directly

Approach

- We engaged known candidate pools in Melbourne as this was the preferred location
- This role required end to end scoping and delivery of consulting work- we assessed communication skills more heavily as a result
- We also scheduled a weekly catch up call to update on our search progress

Outcome

- Talenza was engaged on an exclusive arrangement due to our close ties to industry and our strong network
- Shortlist of 2 presented within 1 week.
- Due to the calibre of shortlist, additional head count created to present an offer to both candidates.



GRC & Architecture Insights

Sydney | Melbourne | Brisbane



GRC & Architecture



We saw a flattening of demand for GRC and security architecture in the first half of FY2022. Our Queensland team saw an uplift in demand in the second half of the FY, we believe this was driven by the SOCI act changes.

Security Awareness is an area we expect to see a lot of growth in this year, the industry is maturing as a whole and we are seeing this role come up more and more.

GRC talent quite flat overall with 2% growth, however a huge churn within consultancies this year, this was prior to the tax fallout for PwC in May 2023. We suggest this is due to people being over utilised and burnt out in consulting and wanting to experience in house.

Boutique consultancies offering GRC services are pushing more heavily into the space also potentially attracting big 4 types. We expect to see more of this over the coming 12 months with consulting work being spread across more companies.

We predict a huge uplift in demand for GRC talent this year due to the high profile breaches we have seen. Legislation changes around the Privacy Act, SOCI Act and APRA CPS234/230 will drive additional demand for talent pools.



Summary of **talent** in this space

1.3 years

Median Tenure

Diversity

21% Female

79% Male

Consultancies losing
staff to industry

25-40%

attrition

1% growth

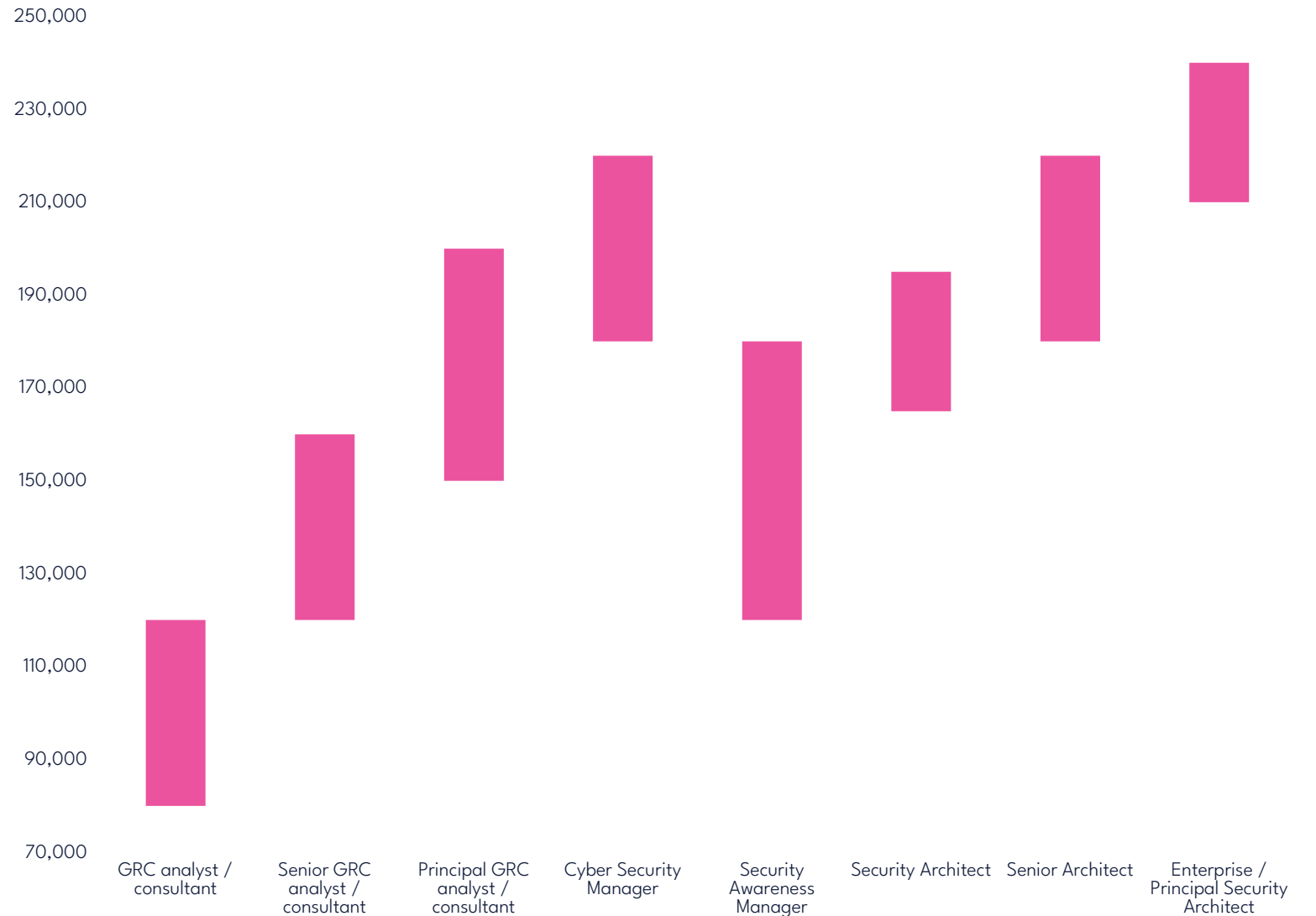
Very flat

Governance Risk and Compliance Architecture



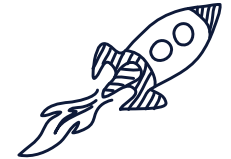
The pink boxes represent the base salary range for each role.

For example, our observed GRC analyst / consultant base salary sits between \$80K - \$120K.



Disclaimer: The data provided in this guide is sourced from information gained by Talenza over the past 12 months recruiting 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. 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. Talenza do not hold any liability for the accuracy of this information.

Case Study: GRC Consultant



Challenge

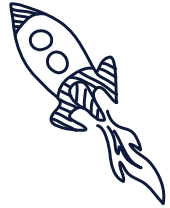
- ASX200 financial service business, preparing for their CPS 234 tripartite audit
- Previously this role was advertised as permanent with multiple candidates declining the offer
- There was a significant time pressure as the audit date was approaching, as a result a contractor was required

Approach

- Our Brisbane and Sydney team worked together to source candidates
- Very targeted search for available contractors nationally with relevant experience
- We engaged existing talent pools and asked for referrals for candidates not visible on SEEK or LinkedIn

Outcome

- Talenza presented an initial shortlist within a week, with the preferred candidate declining the offer
- A replacement candidate was sourced and submitted within 48 hours of briefing
- Contract issued within 7 days of the initial briefing



Case Study: GRC Consultant

Challenge

- Start up style security consultancy offering very niche GRC work
- The company had been looking directly for over 6 months for suitable candidates
- As a start up style business cultural fit was very important

Approach

- A deep search was conducted across the Sydney GRC market, this was during a boom time in the sector
- As the GRC work was deeper than audit and compliance, we assessed based on critical thinking
- Screened against cultural fit through video assessments

Outcome

- A very targeted short list was sent across within a 2 week period
- The preferred candidate was known in our network and had incredible references
- The whole process took less than 4 weeks from briefing to contract signed

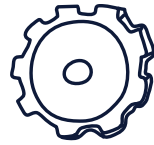


Leadership



Sydney | Melbourne | Brisbane

Leadership



Are we seeing a shift away from the CISO being from a deeply technical background? We have noticed more of a shift to the CISO who can speak business better than can speak technical.

As the industry continues to mature, we believe this will become more and more the norm, similar to what has happened with the CIO and CTO roles in Australia.

With all of the high profile breaches and changes to legislation, we are hearing a lot more board interest and involvement in cyber. The question I have heard from clients has been the board asking if they are safe against a Optus style breach – in a lot of instances they are not.

Budgets to combat the risks are slowly becoming available, however we have not yet seen a huge spike on budgets and team sizes as yet.

We have noticed a trend from several CISO's moving into vendor land over the last few years. We believe this is a combination of escaping the requirement for operational support and the significant salaries on offer.

We've spoken to a number of CISO's who are questioning the value of having cyber insurance due to the rising costs for renewals. It's been likened to a necessary evil in some ways and it is still seen as a must have.

Our opinion is that strong controls and a sound cyber awareness policy is equally important.

Based on data we have seen from a leading breach response firm, the most common attacks over the last 12 months have been Ransomware and Business Email Compromise attacks.

This further highlights the need for a good cyber awareness program and we predict we will see this become a larger portion of budgets.

Our hope and presumably the hope of all CISO's is that with additional pressure on the board from media cyber budgets and headcounts will grow.



Summary of **talent** in this space

2.4 years

Median Tenure

Diversity

16% Female

84% Male

Talent source

- **Charles Sturt University**
- **UNSW**
- **RMIT**

18%

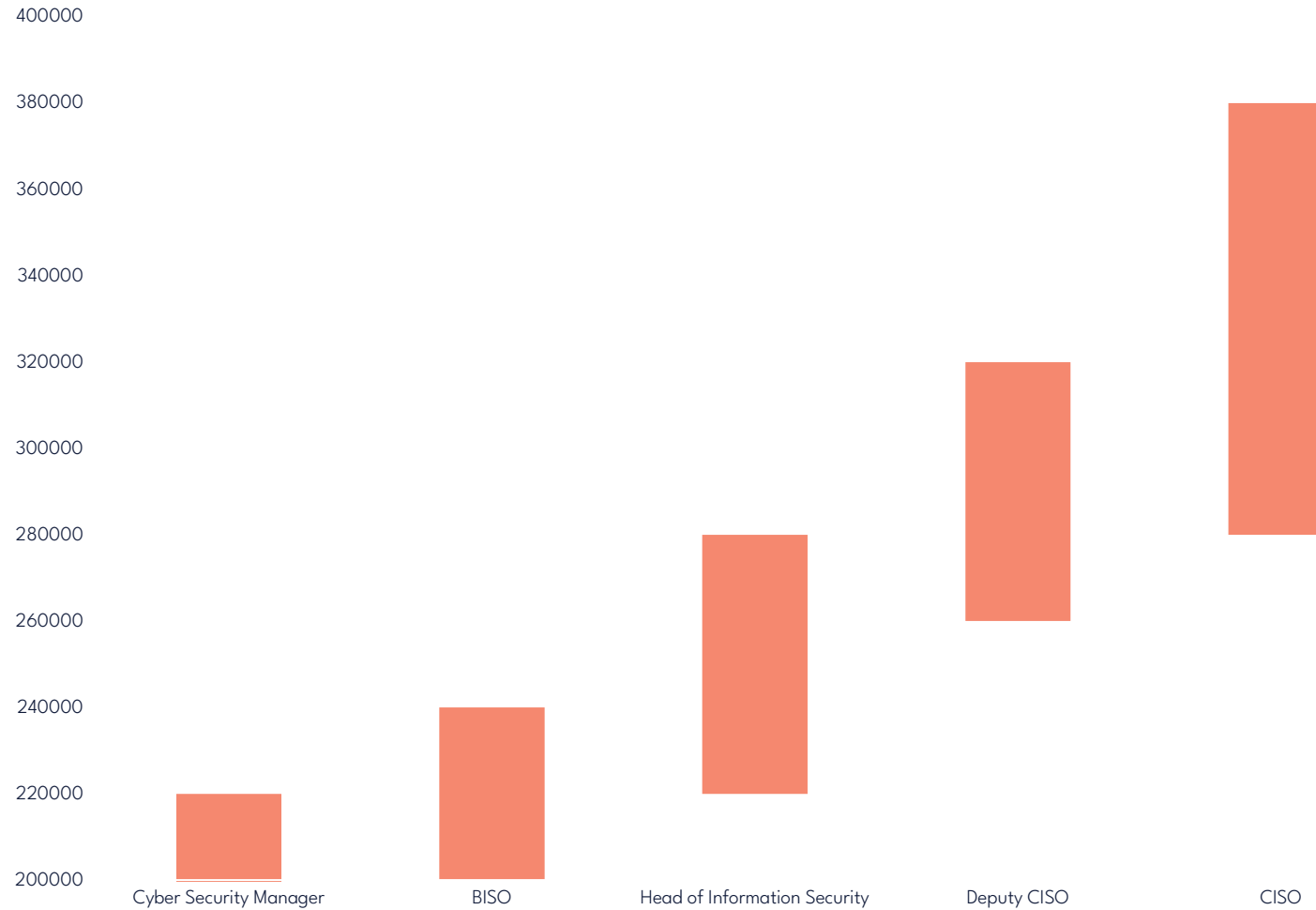
changed roles

Leadership Base Salary Range

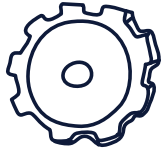


The orange boxes represent the base salary range for each role.

For example, our observed BISO base salary sits between \$180K - \$220K.



Disclaimer: The data provided in this guide is sourced from information gained by Talenza over the past 12 months recruiting 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. 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. Talenza do not hold any liability for the accuracy of this information.



Case Study: CISO

Challenge

- ASX200 financial service business, their outgoing CISO had a short notice period (4 weeks)
- There was an upcoming board meeting, with a high pressure and fast-tracked process.
- This was a fairly immature cyber function, where leadership was very important

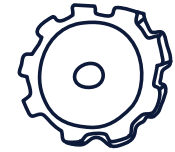
Approach

- Due to the regulatory nature of the business, we were working from a pool of existing CISO's from F/S businesses
- We engaged our known network of CISO's in Sydney and completed a search across the remaining network
- Phone screened, video interviewed to assess against the relevant framework requirements

Outcome

- Initial brief on Wednesday, shortlist of 8 profiles submitted on following Friday.
- Interviews conducted following week, 3 x preferred candidates taken through to advanced interview stages.
- Entire process finalized within 4 weeks of initial briefing.

Case Study: Head of SOC



Challenge

- Leading Managed Security Service Provider hiring a newly created role
- This role was to take on the leadership responsibility and allow the current head of to focus on client acquisition
- High growth team, from 4 to 28 in a 24 month period with combination of technical and leadership skills required

Approach

- Complete search across Sydney and Melbourne markets
- This included in house and services side candidates
- We screened by phone initially for leadership and technical before a follow up video interview

Outcome

- We were engaged exclusively, a shortlist of 5 presented.
- All were interviewed, with a tough decision between the top two candidates for the client.
- Whole process was 3 weeks from brief to offer.



Getting started in **security**



Sydney | Melbourne | Brisbane



Getting started in security



Unfortunately, most of our clients do not utilise our services to hire recent graduates, in more instances internal talent and HR teams manage this process.

Our consultants field numerous calls and inquiries from job searchers in this experience level, the following information can be used as a guide – reach out directly to discuss in more detail.

Cyber is an area where ALL learning and study is valuable to help you land a job BUT there is no singular certification that will instantly result in a job offer.

Most hiring managers want to see a consistent commitment to continuous learning as that is what it takes to keep up to date in an ever evolving industry. In order to land a job it's a mixture of hard work, persistence and a little bit of luck!



Where to start



01

NICE framework

There is a very good framework put together by AusCyber called the NICE framework, it is an excellent starting point to gain insights into the different areas in cyber, identify which skills are valuable and identify roles in each area.

[AusCyber](#)

02

Security Certification Roadmap

Once you've found an area you are interested in, begin/continue to study within that area. On the following link, there is a great resource showing various certification pathways and what roles the skills learned sit within.

[Roadmap](#)

03

Free Training

Learning and development doesn't need to cost you a fortune, there are a whole host of free certifications which can be just as valuable - here's a consolidated list of free training put together by John Amador

[LinkedIn Post](#)

04

Bootcamp Programs

There are a number of bootcamp style programs now being offered, the University of Sydney are offering a 24-week boot camp, Institute of Data also offer a bootcamp style course. Similar to the above courses, you cannot expect you will get a role instantly once completing one of these programs/courses.

You've finished studying, what now?



Graduate Programs

There are a number of existing graduate programs we know of, if you are a current university student most likely there is some internal knowledge and contact points for these programs.

Here is a list of some of the graduate programs we are aware of:

- Deloitte
- KPMG International (KPMG)
- PricewaterhouseCoopers (PwC)
- Ernst & Young (EY)
- Westpac, IAG
- Macquarie Group
- Commonwealth Bank
- NAB
- Telstra
- CyberCX

Monthly Events

Some of the events we are aware of that run on a monthly basis are listed below.

- **SecTalks** – generally monthly in major cities and have great technical topics
- **AISA** - tend to be monthly events, very varied topics of conversation with more of a corporate spin
- **OWASP / AppSec Australia** – Application Security and Offensive security focused meetups

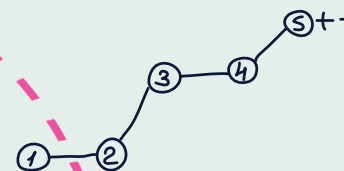
Annual Events

- **Bsides** – runs in most large cities in Australia, these will generally have 300-3000 attendees, Canberra being the largest which as of 2023 will have a day devoted to junior level industry members
- **Hack.Sydney** – first event 2022, this has dedicated free tickets for university student
- **CrikeyCon** – Brisbane based event, excellent close knit community run event (on hiatus in 2022)
- **TuskCon** – Small community event with a limited amount of tickets available



About Us

Sydney | Melbourne | Brisbane





What we have been up to

Sponsored Events

NSW/ACT

- Bsidess Sydney
- OWASP Sydney

QLD

- BSIDES Brisbane
- CrikeyCon
- SecTalks Brisbane
- AWSN Brisbane
- TuskCon



Guest Speaker Events

NSW/ACT

- Hack.Sydney
- OWASP Sydney

QLD

- CISO Brisbane
- AWSN Brisbane



Attended Events

NSW/ACT

- SecTalks Sydney
- AISA SydSec
- OWASP Sydney

QLD

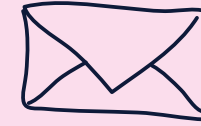
- SecTalks Brisbane
- AISA BrisSEC

Talenza Cyber can deliver



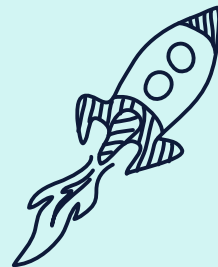
81%

of roles were retained or exclusive to Talenza Cyber



2.75

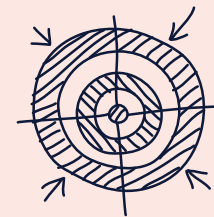
CVs sent per exclusive role



More than

1 in 2

CVs sent on exclusive roles are placed



38%

were golden bullet placements. Meaning the 1st CV sent got the job

What client & candidates say about us

Chelsey Costello

“Chelsey is an exceptionally talented recruiter. She is persistent with her engagements and genuinely interested in knowing more about the role, the hiring manager and organisation. She devotes a lot of time and energy in understanding what the client really wants. Chelsey's dealings are fair to both the client and candidates, creating a very conducive environment for hiring. She has a knack for unearthing really solid profiles in an island continent suffering from an artificial scarcity of cybersecurity talent.”

- Hiring Manager

Riki Blok

“Riki is a first class recruiter and person. Riki definitely takes the time to understand what you are looking for in a role and your career. You are definitely not just another resume to fill his quota, and you feel like he is working for you just as much as he is working for the company paying him.”

- Principal Security Analyst

Brittany Buswell

“There's a reason Brittany is the first person I talk to when I need a specialist Cyber resource. Brittany is knowledgeable, passionate and very well connected in the Cyber space, and always hits the brief when identifying suitable candidates. I've had the pleasure of working with Brittany for many years, across many organisations and Brittany's ability to consistently provide high calibre candidates who also fit the team and organisation are second to none.”

- Hiring Manager



How you can engage us



Due to our specialized search process, we find most clients engage with us on a **retained or exclusive basis**.



This allows us to canvas the whole market – passive and active candidates to present our **qualified shortlist**.



Our **processes** will include a combination of phone calls, VC or in person interviews when selecting candidates for presentation.



We focus on presenting a **high-quality shortlist** without the candidates you don't need to see on it.

Let's chat!

Chelsey Costello



0478 100 161



chelsey@talenza.com.au

Riki Blok



0426 177 613



riki@talenza.com.au

Brittany Buswell



0415 550 810



brittany@talenza.com.au