Cybersecurity

Salary & Insights Report
2025-2026

#BuildingTrust

TECH & DATA PEOPLE
part of SEARCH4

Who are Tech & Data People?

Tech & Data People (TDP) is a specialist provider of Technology and Data Analytics recruitment services in Australia.

With a dedicated team of experienced recruiters and an industry-leading network of professionals, we pride ourselves on connecting top talent with leading organisations across Australia.

Leveraging a combined 100+ years in Technology and Data recruitment, our compassion and understanding for candidates and employers show in our unrivalled network.

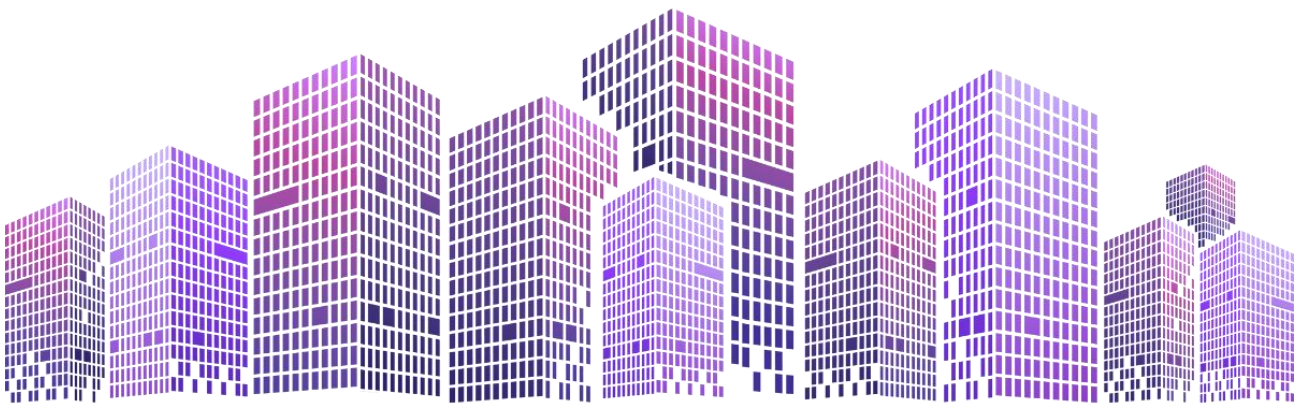
We connect progressive businesses with exceptional contract and permanent talent across the full spectrum of technology roles:

About This Guide

This guide provides a comprehensive overview of the current landscape within the Data Analytics & Business Intelligence sector, with detailed insights into remuneration and recruitment trends across Melbourne, Sydney, Brisbane, and Perth.

Drawing on the expertise of our specialist recruiters and advanced data tools, we've compiled key information on salary benchmarks, contract rates, tenure patterns and gender distribution. These insights are designed to help employers make informed hiring decisions and to support professionals in understanding their market value.

All figures represent benchmark **base** salaries, **excluding** superannuation, and **candidate day rates**, Data has been sourced through a combination of expert knowledge, historical placement records, industry participation, and online data collection, and reflects averages across a range of business sizes and industries.



Informed. Strategic. Data-driven.
Your recruitment intelligence starts here.

2025-26 Market Overview

STUART GARLAND
Director

The cybersecurity sector is entering a period of accelerated growth, driven by heightened regulation, an increasingly hostile threat landscape, and the rise of AI-fuelled attacks. The market is projected to reach AUD 13.3 billion in 2025 and could exceed AUD 20 billion by 2030, growing at 13–14% CAGR.

Demand for cyber services continues to surge. The services segment — spanning advisory, managed services and incident response — is set to grow from AUD 2 million in 2024 to AUD 3.9 million by 2030. Investment in cybersecurity training is also rising sharply, expected to triple to AUD 462 million by 2030.

This growth is underpinned by an evolving regulatory landscape. Updates to the Security of Critical Infrastructure Act, mandatory ransomware payment disclosures, and broader enforcement powers across APRA, OAIC and ACMA have lifted the bar on cyber governance. More than 220 critical infrastructure organisations are now under direct regulatory scrutiny.

But regulation alone won't drive resilience — capability must catch up. Organisations are under pressure to build internal cyber functions that can meet compliance obligations while proactively defending against emerging threats. This shift is prompting a structural rethink: from relying on outsourced vendors to building lean, agile internal teams with embedded expertise in governance, architecture, incident response, and threat detection. As a result, demand for in-house cybersecurity talent is certainly there and competition for experienced professionals is fierce.

Meanwhile, the threat environment has escalated. Ransomware attacks surged, with 94 reported cases in 2024 and 67 already logged in the first half of 2025. AI-powered phishing, deepfake scams and impersonation attacks are rising exponentially — with over 30 million phishing attempts recorded last year and a 300% spike in ATO-related scam reports. ASIO warns that foreign espionage alone is costing Australia upwards of AUD 18.7 billion annually.

And yet, cyber maturity still lags behind. More than 50% of businesses remain below Essential Eight Level 2, despite increasing investment in tech, cloud and AI.

As risk intensifies, so too does the demand for cyber talent — but the gap between skills needed and talent available is widening. Experienced professionals in cloud security, threat intelligence, GRC and identity management are in critically short supply, and recruitment pipelines are under strain.

This is a hiring challenge but more importantly, it's a strategic risk. The scarcity of experienced cyber professionals is already inflating salaries, extending time-to-hire, and forcing compromises on capability. Specialist roles in cloud security, identity and access management, and threat intelligence are some of the hardest to fill, with senior candidates often fielding multiple offers before they even hit the open market. In a space where minutes matter during an incident, unfilled roles and under-skilled teams aren't just operational issues — they're exposure points.

So, the big question becomes: how will organisations secure their future when they can't secure the talent needed to defend it?

Key Trends & Predictions

EMERGING TRENDS

- **Shift toward in-house capability:** More organisations are building internal cyber teams to reduce vendor dependency and improve incident response agility.
- **Rise of cross-functional roles:** There's growing demand for professionals who can bridge technical and business domains (e.g., Cyber BAs, GRC consultants, and Security Architects with stakeholder engagement skills) as the function overall is now seen as business-critical.
- **Upskilling over hiring:** With limited senior talent available, employers are increasingly investing in training mid-level staff or reskilling existing tech professionals into cyber pathways.
- **AI and automation driving role evolution**: Traditional SOC roles are shifting as AI takes over tier-1 monitoring; future hiring is focused more on threat hunting, AI risk governance and contextual decision-making.

PREDICTIONS

- **Cyber hiring will continue to surge**, with an estimated 30–40% increase in open roles across critical infrastructure, finance and gov.
- **Salary inflation will persist**, particularly for cloud, identity, and architecture roles — with senior specialists commanding $220K+ base salaries.
- **Talent from adjacent fields** (e.g., data, infrastructure, compliance) will be increasingly drawn into cyber, especially through internal pathways.
- **Employers without a talent pipeline strategy** (graduate programs, partnerships, EVP, or targeted headhunting) will struggle to attract top-tier candidates.
- **DE&I in cyber will gain momentum**, with a growing push to diversify talent pools — especially women in security, neurodiverse talent, and veterans.

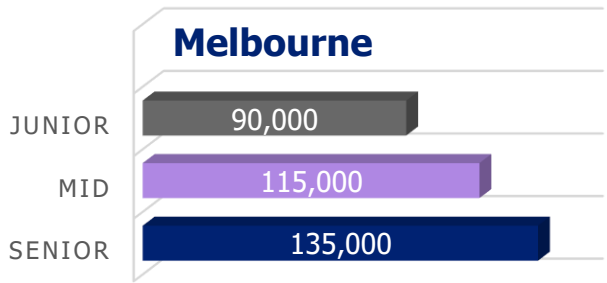
Role Index

Security Administrator

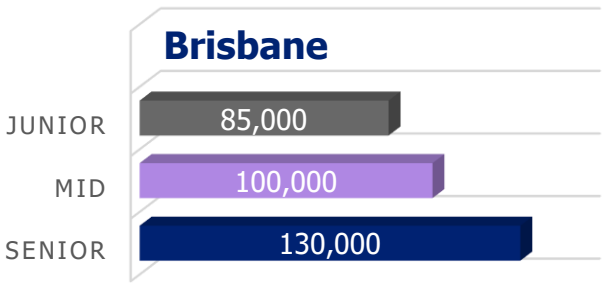
Security Administrators play a critical role in safeguarding access and enforcing policy across increasingly complex environments. As organisations embrace Zero Trust architectures, admins are now central to privileged account management, multi-factor authentication, and access control frameworks across cloud-native and hybrid infrastructures like AWS, Azure and GCP.

The role has expanded beyond traditional perimeter defence. Employers are seeking professionals who can work closely with DevOps, cloud and compliance teams, while bringing experience in automation tools and AI-enhanced monitoring systems. Admins with a proactive mindset and cross-functional skills are in growing demand as security becomes embedded across the entire tech stack.

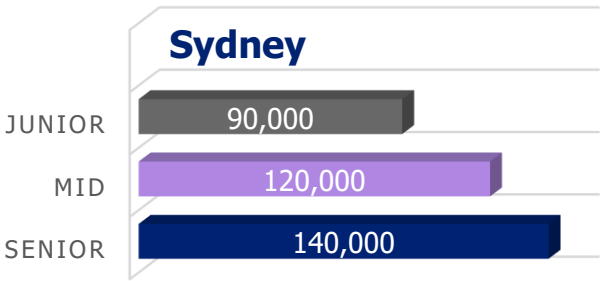
Gender Distribution:	Average Tenure:	Demand:
26% 74%	1.3 years	High



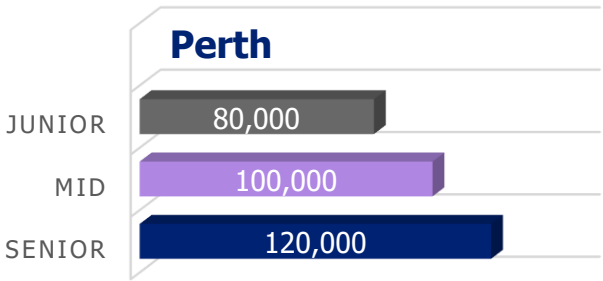
CONTRACT: **$600-$900 Per Day**



CONTRACT: **$600-$850 Per Day**



CONTRACT: **$650-$950 Per Day**



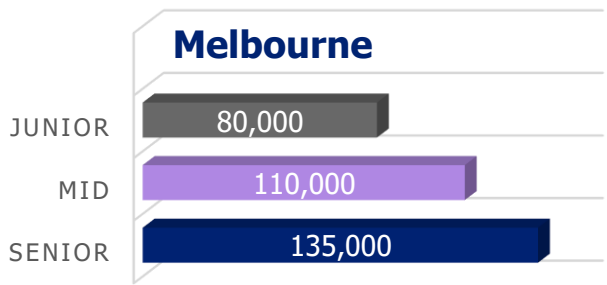
CONTRACT: **$550-$800 Per Day**

SOC Analyst

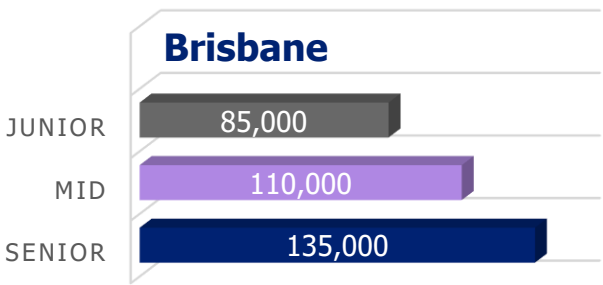
As frontline defenders in the cybersecurity ecosystem, Security Operations Centre (SOC) Analysts are responsible for monitoring, detecting and responding to threats in real-time. With attacks escalating, their role has become more dynamic — requiring not just technical know-how, but the ability to interpret behavioural data, triage incidents quickly and escalate threats with precision.

SOC Analysts are increasingly expected to work across SIEM platforms, threat intelligence tools, and automated response systems. With the rise of AI-enhanced SOCs, employers value candidates who can adapt to emerging technologies, collaborate with incident response and threat hunting teams, and contribute to the continuous improvement of detection rules and response playbooks.

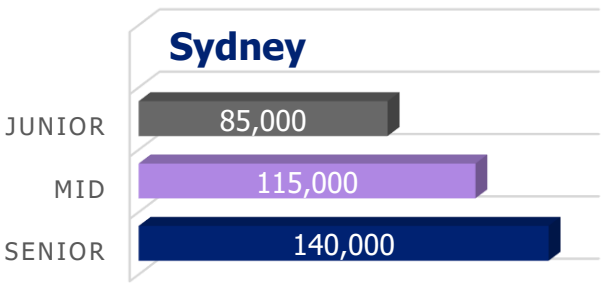
Gender Distribution:	Average Tenure:	Demand:
24% 76%	1.1 years	Very High



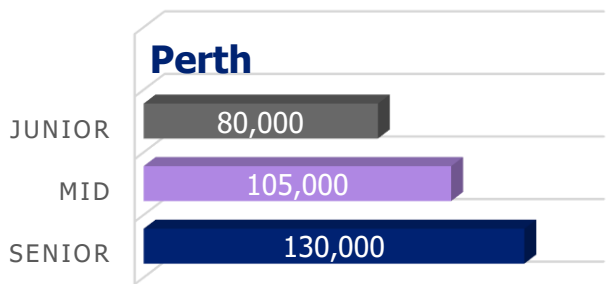
CONTRACT: **$600-$900 Per Day**



CONTRACT: **$600-$850 Per Day**



CONTRACT: **$650-$900 Per Day**



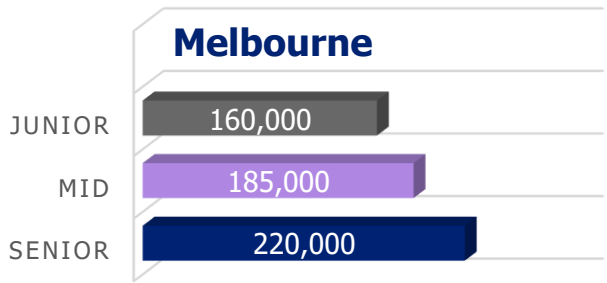
CONTRACT: **$550-$800 Per Day**

Security Consultant

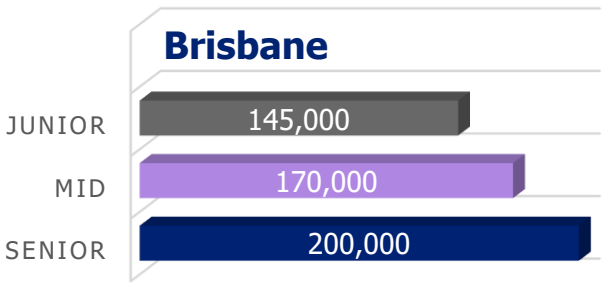
Security Consultants in Australia are becoming key strategic partners in shaping enterprise-wide security posture. Their role goes beyond risk assessments, advising on cloud security architectures, DevSecOps practices and AI-powered threat detection, while aligning solutions with both technical environments and business needs.

As compliance obligations tighten, familiarity with frameworks like ISO 27001, PCI-DSS and the ASD Essential Eight is essential. Consultants who can tailor their approach to industry-specific risks — from finance and healthcare to energy and retail — are in growing demand. Many are also stepping into executive advisory and internal enablement roles, helping drive training, awareness and a security-first culture across the organisation.

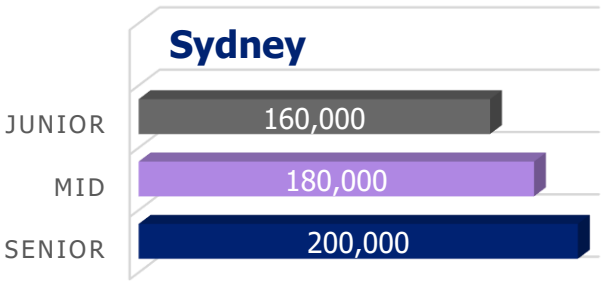
Gender Distribution:	Average Tenure:	Demand:
15% 85%	2.2 years	Very High



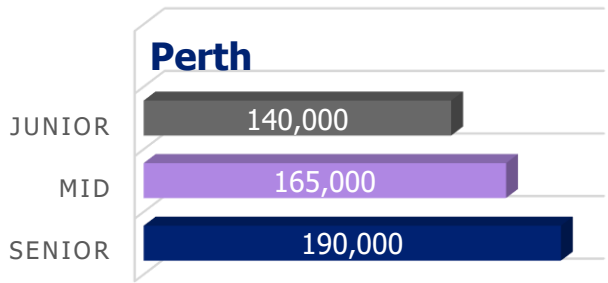
CONTRACT: **$900-$1,375 Per Day**



CONTRACT: **$950-$1,275 Per Day**



CONTRACT: **$900-$1,320 Per Day**



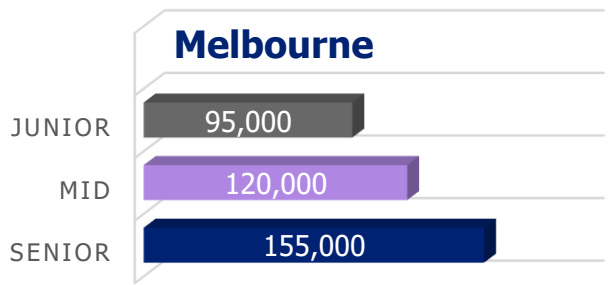
CONTRACT: **$900-$1,250 Per Day**

Governance, Risk & Compliance Analyst

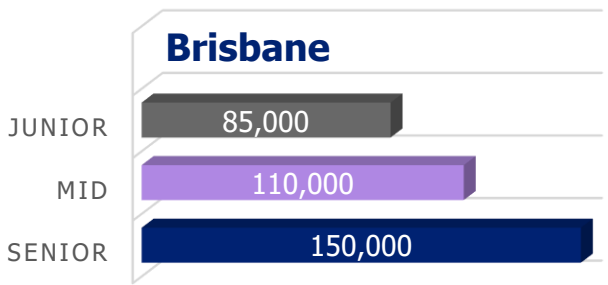
The mounting regulatory scrutiny and rising stakeholder expectations has GRC Analysts emerging as key players in shaping how organisations manage cyber risk. Rather than working behind the scenes, they're increasingly embedded across business units, translating complex security frameworks into actionable policies, risk registers and board-level reporting.

With new legislation, supply chain risk and evolving standards like Essential Eight, ISO 27001, CPS 234 and SOC 2, GRC roles have become more visible and strategic. The strongest analysts blend a sharp eye for detail with an ability to influence — supporting audit readiness, running third-party risk assessments and helping teams operationalise compliance without slowing down innovation.

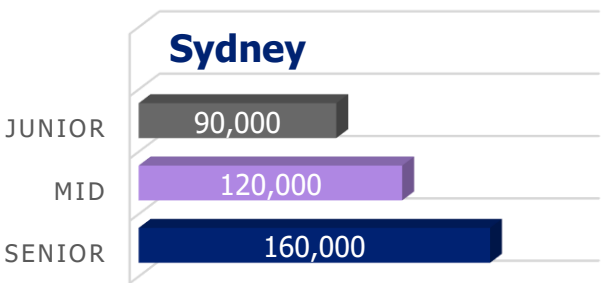
Gender Distribution:	Average Tenure:	Demand:
52% 48%	2.3 years	Very High



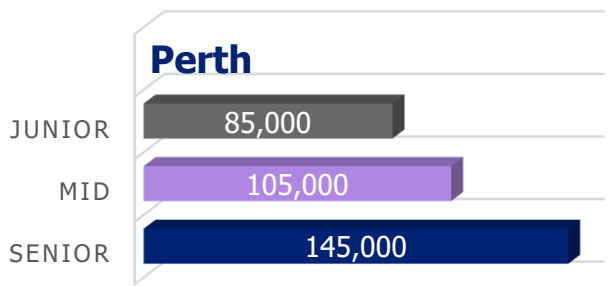
CONTRACT: **$750-$950 Per Day**



CONTRACT: **$700-$950 Per Day**



CONTRACT: **$750-$1,000 Per Day**



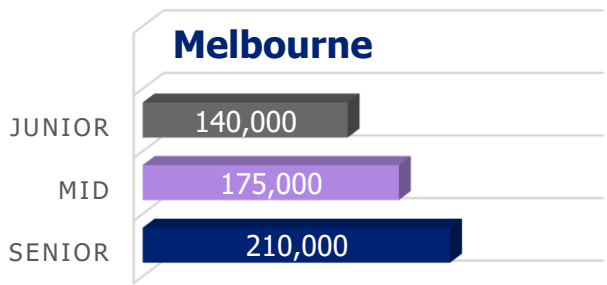
CONTRACT: **$700-$900 Per Day**

Cyber Engineer

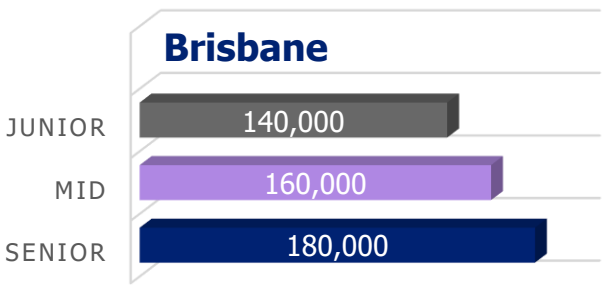
Cybersecurity Engineers are focused on engineering secure-by-design systems from the ground up. With increasing demand for DevSecOps capabilities, container security and CI/CD pipeline protection, engineers are working at the intersection of development and security to harden modern infrastructure at speed.

Compliance is code. Engineers are expected to align technical architecture with regulatory frameworks like ISO 27001, PCI-DSS and the Notifiable Data Breaches (NDB) scheme, while working hand-in-hand with developers, cloud architects, and GRC teams. The role requires deep technical acumen and a collaborative mindset — because security is no longer a checkpoint, it's embedded across the stack.

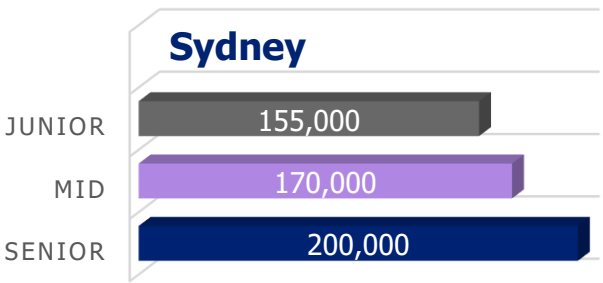
Gender Distribution:	Average Tenure:	Demand:
20% 80%	1.6 years	Very High



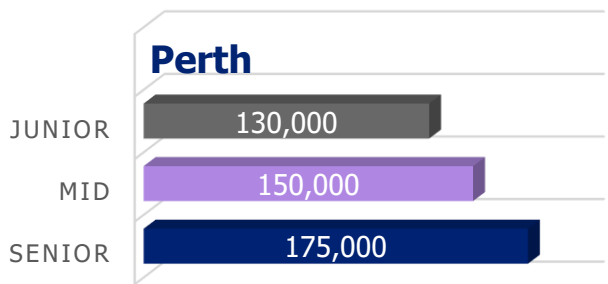
CONTRACT: **$850-$1,150 Per Day**



CONTRACT: **$800-$1,050 Per Day**



CONTRACT: **$850-$1,200 Per Day**



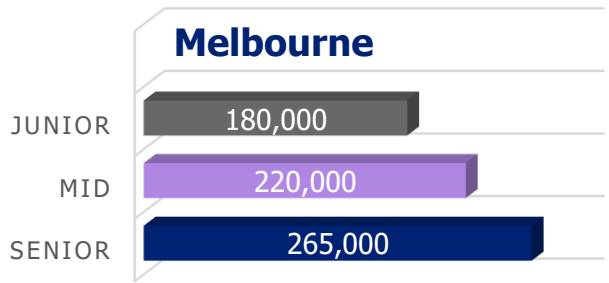
CONTRACT: **$875-$1,000 Per Day**

Security Architect

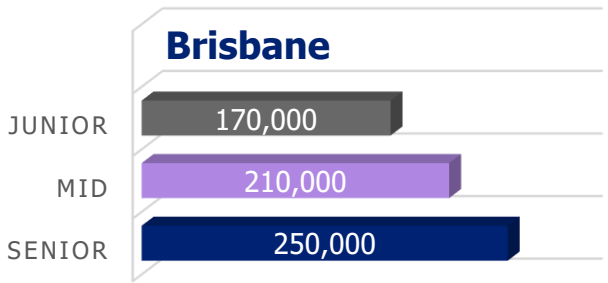
Cyber Architect roles in Australia are evolving into strategic, multidisciplinary positions that bridge technology and business leadership. These professionals serve as trusted advisors to CISOs and executive teams, ensuring security architecture aligns with broader business objectives and risk tolerance. From cloud environments to endpoints, Cyber Architects design comprehensive security frameworks that seamlessly integrate infrastructure, applications, and data layers, enabling resilient and adaptive defenses.

Hiring experienced Security Architects is critical for organisations aiming to proactively manage risk and embed security deeply into their digital transformation efforts.

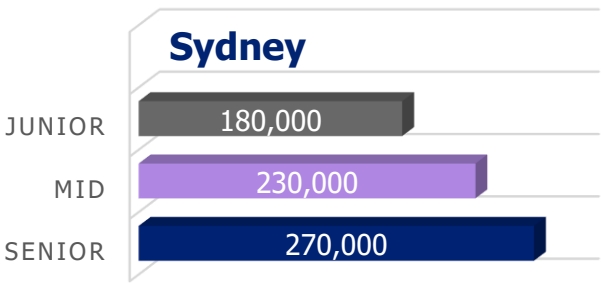
Gender Distribution:	Average Tenure:	Demand:
8% 92%	2 years	Very High



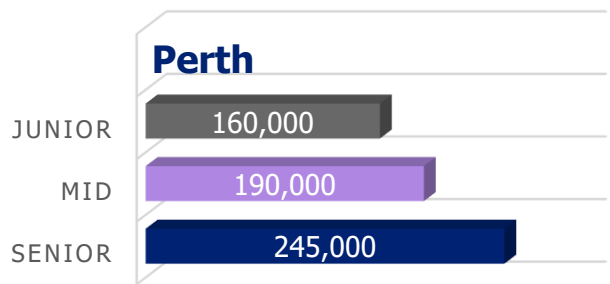
CONTRACT: **$1,150-$1,500 Per Day**



CONTRACT: **$1,050-$1,350 Per Day**



CONTRACT: **$1,100-$1,500 Per Day**



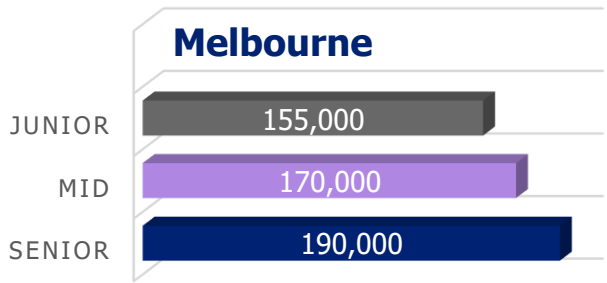
CONTRACT: **$1,000-$1,250 Per Day**

Security Manager

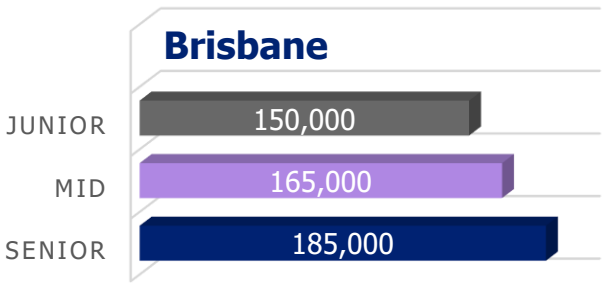
Security Manager positions are increasingly strategic, multidisciplinary and aligned closely with broader business objectives. These leaders contribute to enterprise risk strategy, collaborating directly with executive teams and boards to shape security posture. They oversee security operations centres (SOCs), manage incident response teams, and maintain continuous monitoring and threat mitigation efforts. Additionally, ensuring compliance with key frameworks such as ISO 27001, PCI-DSS, and the Notifiable Data Breaches (NDB) scheme is also in this remit.

Bringing on board forward-thinking Security Managers enables organisations to not only defend against today's threats but also to anticipate and adapt to the shifting cyber risk landscape, embedding security as a business enabler rather than a compliance checkbox.

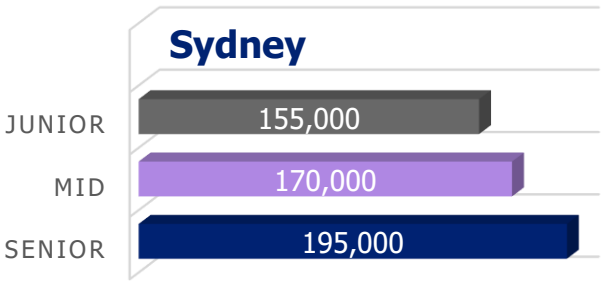
Gender Distribution:	Average Tenure:	Demand:
17% 83%	2.8 years	High



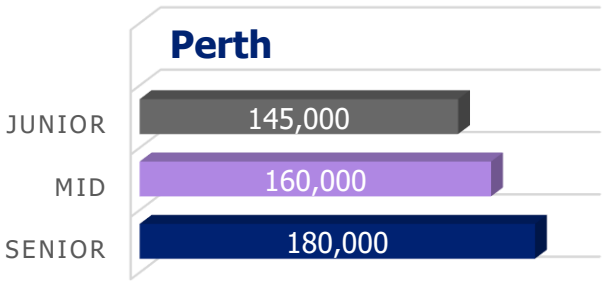
CONTRACT: **$1,000-$1,400 Per Day**



CONTRACT: **$975-$1,300 Per Day**



CONTRACT: **$1,000-$1,450 Per Day**



CONTRACT: **$975-$1,275 Per Day**

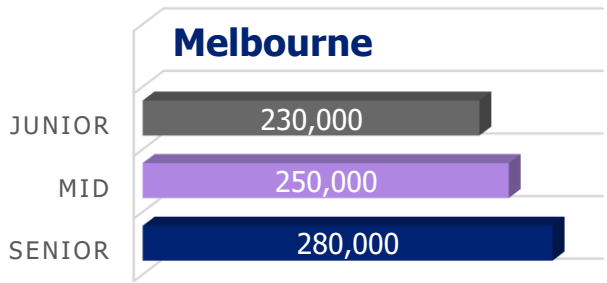
Head of Information Security

Leaders in Head of Information Security roles are tasked with aligning cybersecurity strategy to business goals, innovation roadmaps and digital transformation initiatives.

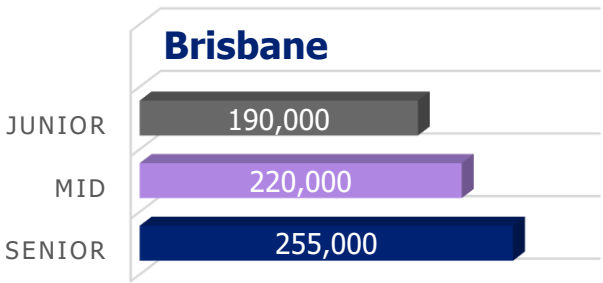
Their remit now spans broader risk management, including regulatory compliance, third-party risk, and operational resilience. These leaders engage directly with boards and executive teams, translating complex technical risks into clear business language to influence strategic decisions.

Visionary leaders who empower organisations to embed security at the core of their business strategy are highly sought after to drive resilience and enable innovation in a rapidly evolving threat landscape.

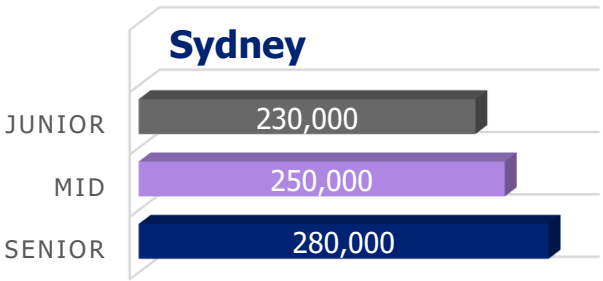
Gender Distribution:	Average Tenure:	Demand:
18% 82%	2.7 years	Very High



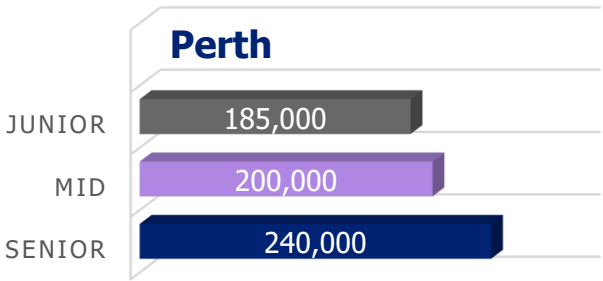
CONTRACT: **$1,200-$1,800 Per Day**



CONTRACT: **$1,050-$1,650 Per Day**



CONTRACT: **$1,200-$1,800 Per Day**



CONTRACT: **$1,050-$1,450 Per Day**

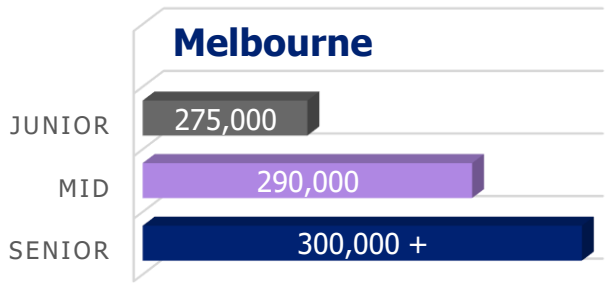
Chief Information Security Officer (CISO)

CISOs today play a pivotal role in shaping enterprise strategy, digital transformation, and risk appetite at the board level. Moving beyond vendor-centric approaches, they focus on identifying capability gaps and crafting cross-functional solutions that leverage open-source and modular technologies.

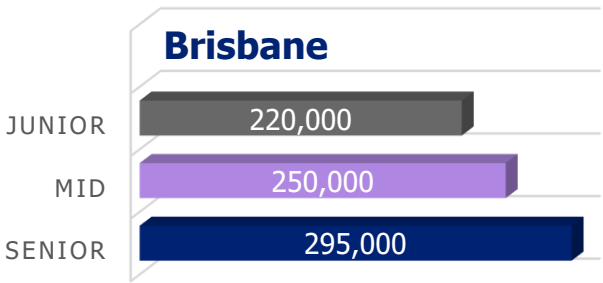
Many CISOs are also spearheading internal AI research, fostering experimentation and continuous learning to proactively address emerging threats and evolving regulatory landscapes.

Successful CISOs act as catalysts for innovation and resilience, embedding security as a strategic enabler that drives business agility and long-term competitive advantage.

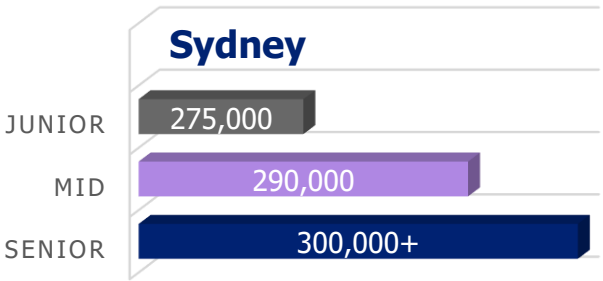
Gender Distribution:	Average Tenure:	Demand:
12% 88%	3 years	Very High



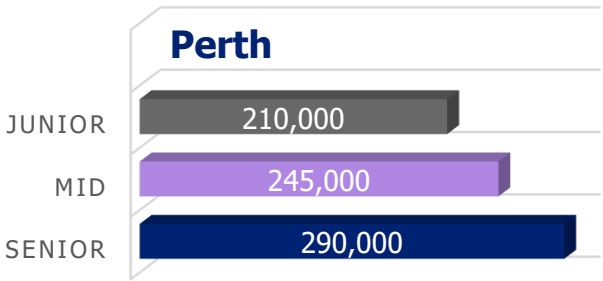
CONTRACT: **$1,400-$2,000 Per Day**



CONTRACT: **$1,250-$1,850 Per Day**



CONTRACT: **$1,400-$2,000 Per Day**



CONTRACT: **$1,100-$1,500 Per Day**

Contact us

Office locations: Melbourne, Sydney, Brisbane, Perth

(03) 8535 3100

info@techanddatapeople.com.au

www.techanddatapeople.com.au

TECH & DATA PEOPLE
part of SEARCH4