# Position Details

## Technical Services- CSOF6

| THE FOLLOWING INFORMATION IS FOR APPLICANTS | |
|---|---|
| **Advertised job title** | Technical Cyber Security Advisor / Penetration Tester |
| **Job reference** | 102720 |
| **Tenure and work schedule** | Indefinite, Full-time<br>We will explore options for part-time, job-share and flexible work arrangements based on needs of the role and individual circumstances. |
| **Salary range** | AU$135,571 - AU$158,863 per annum (pro-rata for part-time)<br>plus up to 15.4% superannuation |
| **Location(s) and office arrangements** | Melbourne (Clayton), Perth (Kensington), Canberra (Black Mountain), Hobart, Brisbane, Sydney (Marsfield) |
| **Relocation assistance** | N/A |
| **Applications are open to** | Australian Citizens Only |
| **Position reports to the** | Cyber Resilience Manager |
| **Client focus – Internal** | 80% |
| **Client focus – External** | 20% |
| **Number of direct reports** | 0 |
| **Enquire about this job** | Contact Abby Breytenbach, via email at Abby.breytenbach@csiro.au |
| **Support and workplace adjustments** | We offer a range of reasonable supports and workplace adjustments. Please let us know via email sarah.lyons@csiro.au if we can help you to equitably participate in our recruitment process or the role itself. |
| **How to apply** | Apply online at https://jobs.csiro.au/<br>Internal applicants please apply via **Jobs Central**<br>If you experience difficulties when applying, please email careers.online@csiro.au |

### Acknowledgement of Country

CSIRO acknowledges the Traditional Owners of the land, sea and waters, of the areas that we live and work on across Australia. We acknowledge their continuing connection to their culture and pay our respects to their Elders past and present. View our vision towards reconciliation.

### About CSIRO

As Australia's national science agency, CSIRO is solving the greatest challenges through innovative science and technology. Many of our iconic innovations were once considered impossible until someone, just like you, joined us and took on the challenge.

As one of the world's largest multidisciplinary mission-driven research organisations, we are focused on the issues that matter the most: for our quality of life, for the economy and for our environment. We believe diverse teams are more effective and deliver more innovative outcomes. When we all focus on the big things that really matter, and work in partnership with our communities and Indigenous Australia, Australian science and technology can solve seemingly impossible problems and create new value for all Australians. Visit CSIRO.au for more information.

## Role overview

As part of CSIRO's Information Management and Technology (IMT), Cyber Security Resilience team plays a pivotal role in protecting CSIRO's information assets to enable achievement of nation's science and research objectives. The key capabilities this team delivers include cyber assurance & advisory, cyber architecture & engineering, third-party cyber risk management, vulnerability management and penetration testing.

CSIRO is looking for a motivated penetration testing lead, to join the Cyber Security Resilience team as a Cyber Security Technical Advisor. This role has no direct reports, but will lead the penetration testing function, coordinate penetration testing and red teaming activities, provide hands-on testing expertise, and uplift organisational capability through mentoring and technical guidance.

The successful candidate will have experience leading or coordinating complex testing engagements across a range of environments and can provide practical security advice and high-quality deliverables through positive, collaborative engagement with key stakeholders.

The candidate will be expected to demonstrate security testing expertise through the analytical investigation of vulnerabilities with known tools and techniques, and to design and execute threat-informed tests (including adversary emulation/red teaming techniques) in line with agreed rules of engagement.

We are seeking an adaptable, analytical and self-motivated candidate who will work well in a fast-paced and complex environment, whilst managing competing priorities under the direction of Cyber Resilience leadership. The role provides technical leadership without direct reports by leading the penetration testing function, coordinating and supporting the work of other team members (and vendors where required), mentoring junior staff, and ensuring findings translate into actionable remediation and measurable uplift in cyber security maturity.

## Duties and key result areas

- Lead the planning and coordination of security testing activities (i.e. penetration testing and red teaming activities, including scheduling, stakeholder alignment, and rules of engagement.
- Perform and oversee penetration tests on web applications, bespoke systems, complex and sensitive infrastructure, and cloud services, ensuring safe execution and minimal operational impact.

- Document, validate and prioritise findings; produce clear, timely reports and briefings that communicate risk, impact, and practical remediation options to technical and non-technical stakeholders.
- Develop and maintain testing methodologies, scoping documents, rules of engagement and repeatable playbooks for environments that do not fit standard IT patterns, including threat-informed and adversary emulation approaches.
- Carry out quality assurance and peer review for testing deliverables, ensuring consistency of evidence, severity ratings, and remediation guidance.
- Stay current with evolving threats, attacker TTPs, and security trends; evaluate and improve tooling and techniques used by the testing function.
- Partner with vulnerability management, cyber architecture/engineering and detection/response teams to validate risk, support remediation, and uplift defensive controls through purple-team style collaboration.
- Provide technical leadership without direct line management by guiding prioritisation, coordinating stakeholders, and recommending pragmatic risk treatment options aligned to business needs.
- Facilitate engagement readouts and communicate openly, effectively and respectfully with all staff, clients and suppliers in the interests of good business practice, collaboration and enhancement of CSIRO's reputation.
- Work collaboratively as part of a multi-disciplinary, regionally dispersed team, mentoring junior staff through coaching, pairing and review to uplift penetration testing and red teaming capability.
- Working with Children/Vulnerable People checks (WWC/VP check) might be required for projects working with children or young people.
- Adhere to the spirit and practice of CSIRO's Values, Code of Conduct, Health, Safety and Environment procedures and policy and diversity initiatives.
- Other duties as directed.

## Selection criteria

### Essential

*Under CSIRO policy only those who meet all essential criteria can be appointed.*

1. 4+ years of hands-on experience in penetration testing (or similar), including coordinating end-to-end engagements (scoping, execution, reporting) and working effectively across multiple stakeholders.
2. Understanding of scripting languages such as Python, PowerShell and Bash.
3. Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defence-in-depth).
4. Knowledge of application vulnerabilities and experience conducting application vulnerability assessments.
5. Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, malicious code).
6. Demonstrated experience in penetration testing principles, tools, and techniques.
7. Proven capability in executing comprehensive web application testing.

8. Demonstrated ability to mentor and uplift junior testers through coaching, structured feedback, and review of technical deliverables.
9. Experience designing or delivering threat-informed testing (e.g., attack simulation, adversary emulation, or red team techniques), with a strong focus on safety, authorisation and clear rules of engagement.
10. OSCP/GPEN/OSWE/CRTO equivalent certification or relevant industry experience.
11. Excellent reporting, presentation and communication skills, including the ability to brief executives, facilitate technical deep-dives, and drive remediation discussions.

**Desirable**

1. Experience with threat hunting, detection engineering, or purple teaming to validate and improve defensive controls.
2. Perform code analysis services to identify potential security issues.
3. Technical experience reviewing the security configuration of on-premises and/or cloud-based enterprise technologies.
4. Experience with OT and IoT environments.
5. Experience in providing mentoring to cyber security staff.
6. Familiarity with:
    a. Mitre Attack Framework.
    b. CVSS 3.1.
7. Experience with cyber security frameworks including Australian Government Information Security Manual (ISM), Protective Security Policy Framework (PSPF) and Essential 8 (E8).

**Not sure if you need all the criteria?**

While it is CSIRO policy that the successful candidate must meet all the essential criteria, there are many ways to demonstrate this. Don't let the list discourage you. If you are unsure about applying, please reach out to the contact on page 1 of this document so we can discuss the role further.

## Required competencies

- **Teamwork and collaboration:** Cooperates with others to achieve organisational objectives and may share team resources in order to do this. Collaborates with other teams as well as industry colleagues.
- **Influence and communication:** Identifies critical stakeholders and influences them via an influential third party, for example through an established network, to gain support for sometimes contentious, proposals/ideas.
- **Resource management/leadership:** Provides leadership that fosters an environment that encourages new ideas and provides support for the development of emerging skills. Creates trust by displaying consistency, understanding, integrity and patience. Plans, seeks, allocates and monitors resources to achieve outcomes.
- **Judgement and problem solving:** Anticipates and manages problems in ambiguous situations. Develops and selects an appropriate course of action and provides for contingencies.

Evaluates, interprets and integrates complex bodies of information and draws logical conclusions, synthesises proposals and defends options with reasoned arguments.

- **Independence:** Assesses the risk and opportunity of identified strategies, options and actions. Overcomes problems and setbacks in achieving goals. Invariably includes consideration of value-added future impact on bottom line when determining the optimal and efficient use of resources.
- **Adaptability:** Demonstrates flexibility in thinking and adapts to and manages the increasing rate of organisational change by adjusting strategies, goals and priorities.

## Setting you up for success

We understand that not everyone works in the same way and sometimes people may require reasonable support and adjustments to perform at their best. Whether related to the recruitment process and or the role itself, this may include options such as providing different methods of communication, flexible hours or physical adjustments to work methods. If you feel comfortable, we encourage you to share any support and adjustments you may need to carry out the inherent requirements of the role. Please let us know via email Sarah.lyons@csiro.au if we can help you to equitably participate in our recruitment process or the role itself

## Life at CSIRO and flexible working arrangements

We work flexibly at CSIRO, offering a range of options for how, when and where you work. We can discuss flexible work arrangements with you during the recruitment process. CSIRO also offers a range of leave entitlements, benefits and career development opportunities. To learn more, visit Careers at CSIRO.

We celebrate the uniqueness of our workforce and are committed to creating diverse and inclusive teams where everyone feels they belong. CSIRO is an equal employment opportunity organisation dedicated to recruiting people based on merit, and reflecting the diversity of the community we serve. We recognise true diversity encompasses all ages, nationalities, abilities, cultures, genders, sexualities, faiths, levels of education, diversity of thought and many more aspects of identity. By empowering diverse teams, our community is reflected in the solutions we create.

## CSIRO values

CSIRO is a values-based organisation committed to values-based leadership.

| Value | Descriptor | Behaviour |
|---|---|---|
| **People first** | Our priority is the safety and wellbeing of our people. We believe in, and respect, the power of diverse perspectives. We seek out and learn from our differences. | • Respectful<br>• Caring<br>• Inclusive |
| **Further together** | We achieve more together than we ever could alone. We listen and collaborate, in teams, across disciplines, across boundaries. We embrace ambiguity and use discussion and | • Accountable<br>• Authentic<br>• Courageous |

| | | |
|---|---|---|
| | persistence to generate unique solutions to complex problems. | |
| **Making it real** | We do science with real impact. We thrive when taking on the big challenges facing the world. We take educated risks and defy convention. We celebrate successes and failures and leverage them to learn as we strive to be the force for positive change. | • Partnering<br>• Cooperative<br>• Humble |
| **Trusted** | We're driven by purpose but remain objective. We fight misinformation with facts. We earn trust everywhere through everything we do. We trust each other and we hold each other accountable. Together our actions drive Australia's trust in CSIRO. | • Curious<br>• Adaptive<br>• Entrepreneurial |

## Child safety

CSIRO is committed to the safety and wellbeing of all children and young people involved in our activities and programs. View our Child Safe Policy.

## Special requirements

Appointment to this role is subject to provision of a pre-employment background check and may be subject to other security/medical/character clearance requirements.

- The successful candidate will undertake a pre-employment background check. Please note that individuals with criminal records are not automatically deemed ineligible. Each application will be considered on its merits.
- The successful candidate will be required to obtain and maintain a security clearance at the Negative Vetting level 1.