# Position Details

## Technical Services- CSOF6

| THE FOLLOWING INFORMATION IS FOR APPLICANTS | |
|---|---|
| **Advertised Job Title** | Senior Technical Advisor – Penetration Testing |
| **Job Reference** | 98487 |
| **Tenure** | Indefinite |
| **Salary Range** | Negotiable |
| **Location(s)** | Sydney (Lindfield), Melbourne (Clayton), Canberra (Black Mountain), Brisbane (St Lucia), Adelaide & Hobart |
| **Applications are open to** | Australian Citizens Only |
| **Position reports to the** | Cyber Assurance Lead |
| **Client Focus – Internal** | 85% |
| **Client Focus – External** | 15% |
| **Number of Direct Reports** | 0 |
| **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.

### 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.

### 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.

The CSIRO Cyber Security Resilience team is seeking a highly skilled Senior Technical Advisor (Penetration Tester). The candidate will be responsible for conducting comprehensive penetration testing engagements across our network infrastructure, applications, and cloud environments. This role demands a deep understanding of security best practices, advanced exploitation techniques, and a passion for uncovering vulnerabilities across multiple layers of technology and the defence mechanisms associated with them.

The candidate will have experience in balancing the cyber security requirements with CSIRO's scientific business requirements, and CSIRO's cyber security risk posture.

The candidate will have experience across a broad range of industries and can demonstrate subject matter expertise in providing technical testing and assurance capabilities to organisations, through positive collaborative engagement with key stakeholders.

This candidate will need to be self-motivated, work well under pressure in a fast-paced and complex environment whilst managing competing priorities under the direction of Cyber Security Resilience leadership. The candidate must be able to demonstrate how they have supported organisations to identify vulnerabilities via security testing and provide remediation recommendation, in coordination with relevant parties, leading to increased cyber security maturity.

## Duties and Key Result Areas

The role will provide the following capabilities:

- Plan, execute, and document penetration testing engagements against internal systems, applications, and cloud environments.
- Identify, exploit, and report critical vulnerabilities using various penetration testing methodologies and tools.
- Develop and execute custom exploits and attack vectors to bypass security controls.
- Analyse vulnerabilities, assess their impact, and prioritise remediation efforts.
- Develop and deliver technical reports outlining findings, recommendations, and proof-of-concept exploits.
- Stay up to date on the latest security threats, vulnerabilities, and attack techniques.
- Participate in internal security initiatives and collaborate with other security teams.
- Contribute to the development and improvement of internal security processes and tools; and
- Develop other security deliverables as directed

## Selection Criteria

### Essential

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

1. Demonstrated 5+ years' experience in penetration testing (enterprise networks, web applications, and phishing).
2. Demonstrated experience in technical security operations
3. Demonstrated experience in scoping business areas for security analysis/testing.
4. Demonstrated experience in report writing, and peer review/quality assurance.

5. Excellent presentation skills plus ability to talk to all levels of staff including Executive and ability to persuade and influence.
6. Excellent interpersonal, collaboration, and communication skills along with the ability to apply initiative, autonomy, quality of work, and teamwork; and

**Desirable**

1. OSCP (Offensive Security Certified Professional) certification
2. Experience in providing mentoring to cyber security staff.
3. Experience in contributing to the development of security-supporting policies, procedures, standards and guidelines

## 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.

## Special Requirements

Appointment to this role may be subject to conditions including provision of a national police check as well as other security/medical/character clearance requirements.

- This position requires a Negative Vetting 1 level security clearance. The successful candidate will be required to obtain a NV1 clearance.

## About CSIRO

We solve the greatest challenges through innovative science and technology. Visit CSIRO Online for more information.

CSIRO is a values-based organisation. In your application and at interview you will need to demonstrate behaviours aligned to our values of:

- People First
- Further Together
- Making it Real
- Trusted