Position Details

Technical Services - CSOF5

THE FOLLOWING INFORMATION IS FOR APPLICANTS	
Advertised Job Title	Senior Test Analyst (Cyber Security)
Job Reference	100943
Tenure	12 Months Term , Full-time
Salary Range	AU$ 114,219 - AU$ 123,605 per annum (pro-rata for part-time) plus up to 15.4% superannuation
Location(s)	All main CSIRO locations
Relocation Assistance	Will be provided to the successful candidate if required
Applications are open to	Australian Citizens Only
Position reports to the	Supervisor – Test Centre of Excellence
Client Focus – Internal	100%
Client Focus – External	0%
Number of Direct Reports	0
Enquire about this job	Contact Radhish Kumar Soundararajan via email at Radhishkumar. Soundararanjan@csiro.au
How to apply	Apply online at https://jobs.csiro.au/ Internal applicants please apply via **Jobs Central** If you experience difficulties when applying, please email careers.online@csiro.au or call 1300 984 220.

Role Overview

As a Senior Functional Test Analyst within CSIRO's Information Management and Technology (IMT) business unit, you will play a pivotal role in delivering quality assurance across a growing and ambitious portfolio of cyber security initiatives. You will lead a range of testing activities within a fast-evolving environment that values adaptability, continuous improvement, and technological innovation.

CSIRO is seeking to appoint a Senior Functional Test Analyst to support the implementation and ongoing assurance of new and existing cyber security capabilities. These may include threat detection and response platforms, identity and access management systems, secure information sharing tools, and security monitoring and reporting solutions.

Your testing responsibilities will span functional, regression, system, security, and integration testing ensuring solutions are robust, secure, and aligned with CSIRO's cyber resilience objectives. You will be responsible for creating detailed test strategies and plans, executing tests, and producing actionable test reports to accompany key cyber product releases.

You will also contribute to building the test practice across our cyber security program, supporting and mentoring other analysts and helping to shape the strategic direction of the testing discipline within the security domain.

Working in an agile, interdisciplinary environment, you will collaborate with security architects, analysts, developers, system engineers, product owners, and executive stakeholders. Your ability to work independently, think critically, and lead quality initiatives will be key to ensuring high confidence in the delivery of secure and reliable solutions.

To succeed, you'll need to be comfortable with ambiguity, welcome change, and value working solutions over rigid processes. Your leadership and testing expertise will directly support CSIRO's mission to protect its people, information, and infrastructure in an increasingly complex digital landscape.

Duties:

- **Lead Testing Activities**: Oversee and manage functional, regression, system, integration, and cyber security testing activities, ensuring thorough and effective validation of software against security requirements and threat models.

- **Cyber Security Test Design**: Develop and execute test cases and scenarios focused on security aspects such as vulnerability assessments, penetration testing, secure code reviews, and compliance validation.

- **Strategic Planning**: Develop and implement detailed plans to describe, explain, and schedule the anticipated testing approach, including security testing strategies, aligning with organisational risk management and strategic goals.

- **Reporting**: Produce comprehensive test reports in tandem with key product releases, including security test findings, risk assessments, and mitigation recommendations for stakeholders.

- **Capability Building**: Take responsibility for building the capability of test analysts, providing mentorship and guidance in security testing methodologies, tools, and best practices.

- **Innovation and Improvement**: Foster a culture of continuous review and improvement, encouraging innovation and the adoption of best practices in both functional and security testing domains.

- **Collaboration**: Work closely with interdisciplinary teams including testers, developers, business analysts, infrastructure specialists, cyber security professionals, data librarians, executive managers, and other stakeholders to ensure cohesive and effective collaboration.

- **Leadership**: Demonstrate initiative, leadership, and independence in managing testing activities, particularly in security-critical projects, driving the team towards achieving strategic objectives.

Key Result Areas:

- **Effective Testing Management**: Successful oversight and management of all testing activities, including security testing, ensuring high-quality, secure, and reliable software products.

- **Strategic Alignment**: Development and execution of testing plans that align with the organisation's strategic and operational objectives, including cyber security risk management.
- **Comprehensive Reporting**: Delivery of detailed test reports that provide clear insights and recommendations, including security vulnerabilities and risk mitigation strategies, contributing to informed decision-making.
- **Team Development**: Enhanced capability and performance of test analysts through effective mentorship and leadership, with a focus on security testing skills and awareness.
- **Continuous Improvement**: Implementation of innovative practices and continuous improvement initiatives that enhance both functional and security testing processes and outcomes.
- **Collaborative Success**: Effective collaboration with interdisciplinary teams, including cyber security experts, resulting in cohesive and successful project outcomes.
- **Leadership Impact**: Demonstrated leadership and independence, driving the team towards achieving strategic goals and objectives, particularly in security-sensitive environments.

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:** Uses knowledge of other party's priorities and adapts presentations or discussions to appeal to the interests and level of the audience. Anticipates and prepares for others reactions.
- **Resource Management/Leadership:** Sets up and maintains effective and efficient work teams and manages performance and resources, to achieve objectives. Chooses appropriate management strategies and communication styles to maintain high levels of motivation and productivity. Gives feedback for development purposes and provides support and direction for improvement.
- **Judgement and Problem Solving:** Investigates underlying issues of complex and ill-defined problems and develops appropriate response by adapting/creating and testing alternative solutions.
- **Independence:** Plans, sets and works to meet challenging standards and goals for self and/or others. Recognises where endeavours will make the most impact or difference, decides on desired outcome and sets realistic goals to reach this target.
- **Adaptability:** Copes with ambiguity or situations that lack clarity. Adapts readily to changing circumstances and new responsibilities (which may include activities outside own preferences) in the interests of achieving team objectives. Recognises the need for and undertakes personal development as a result of changes.

Selection Criteria

Essential

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

- **Extensive Experience**: A minimum of 8 years' experience in testing software applications, including at least 2 years in cyber security testing, coupled with relevant tertiary qualifications in IT or equivalent relevant work experience.
- **Advanced Knowledge**: Demonstrated advanced knowledge and extensive experience in testing analysis techniques, processes, and methodologies, including security testing approaches such as vulnerability assessment, penetration testing, and secure code review.
- **Comprehensive Testing Expertise**: Extensive experience in all aspects of testing, including functional, system integration, regression, and security testing, both as a sole testing resource and within a team.
- **Cyber Security Certification**: Possession of or progress toward a recognised cyber security certification such as:
    - Certified Information Systems Security Professional (CISSP) – preferred
    - Certified Ethical Hacker (CEH) or Offensive Security Certified Professional (OSCP) – desirable
- **Agile-Scrum Proficiency**: Demonstrated extensive experience working in and/or exposure to an Agile-Scrum development environment, including secure development practices.
- **Superior Communication Skills**: Excellent communication skills, with the ability to work collaboratively across multi-disciplinary project teams and communicate effectively with staff and clients at all levels, including cyber security stakeholders.
- **Agile Ceremonies Experience**: Proven experience in backlog refinement, sprint review, retrospective, and planning ceremonies, with an understanding of integrating security considerations into Agile workflows.

Desirable:

- Experience testing both front-end and back-end web application systems with
    a. A focus on discovery and access of research data
    b. high throughput requirements for relational & file-based data processing.
    c. significant data scale/magnitude (i.e. Terabytes, Petabytes).
    d. a focus on discovery and access of research data.
    e. Integrations and interfaces with external systems e.g. REST web services
    f. Knowledge/ hands-on experience with NFT tools
- Knowledge or hands-on experience with **Non-Functional Testing (NFT)** tools, including those used for **security testing** (e.g. Burp Suite, OWASP ZAP, Nessus, or similar).
- Familiarity with **secure software development lifecycle (SSDLC)** practices and tools.

Special Requirements

- The successful candidate will be required to obtain and maintain a security clearance at the Negative Vetting Level 1.

About CSIRO:

We solve the greatest challenges through innovative science and technology. To find out more visit us online!