# Position Details

## Technical Services - CSOF5

|  |
| --- |
| The following information is for applicants |
| Advertised Job Title | Senior Cyber Security Analyst |
| Job Reference | 97533 |
| Tenure | Indefinite |
| Salary Range | AU$110,038 - AU$119,080 per annum (pro-rata for part-time)plus up to 15.4% superannuation |
| Location(s) | * Black Mountain - Canberra, ACT
* Pullenvale - Brisbane, QLD
* Lindfield - Sydney, NSW
* Clayton - Melbourne, VIC
* Kensington - Perth, WA
 |
| Relocation Assistance | Will be provided to the successful candidate if required |
| Applications are open to | Australian Citizens Only |
| Position reports to the | Cyber Security Operations Team Lead |
| Client Focus – Internal | 80% |
| Client Focus – External | 20% |
| Number of Direct Reports | 0 |
| Enquire about this job | Contact James Leith via email at james.leith@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. |

**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](https://www.csiro.au/en/about/Indigenous-engagement/Reconciliation-Action-Plan).

**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](https://www.csiro.au/en/about/policies/child-safe-policy).

### Role Overview

### The Cyber Security Operations team operates within the Enterprise Platforms division as part of the wider Information Management & Technology (IMT) business unit, providing ongoing operational monitoring and assurance activities over enterprise security controls across the organisation.

### As a Senior Cyber Security Analyst, you will work in a fast-paced and complex environment whilst managing competing team and individual priorities. You’ll require competence in a multitude of cyber security disciplines with primary responsibilities with the engineering and maintenance of complex enterprise-wide monitoring, threat detection, analytics and reporting services. You will demonstrate expertise in the investigation of complex cyber security events, including the analysis of indicators of compromise, attacks, telemetry data and alerts. You will also contribute to the evolving technical capabilities within the team and undertake professional development supporting the ever-changing cyber security environment.

### Duties and Key Result Areas

* Engineer and implement security controls that integrate and enhance the monitoring, alerting, investigation and threat detection capabilities of the Cyber Security Operations team.
* Design and develop automations/integrations/tooling to enhance the detection and response capabilities of the team.
* Develop detection strategies including attack models, event correlations and use cases, to assist in further tuning detection capabilities and prevent incidents from recurring.
* Design, enhance and maintain the SIEM/SOAR infrastructure and services.
* Maintain, develop and enhance the advanced security control capabilities of the enterprise firewalls, such as threat detection and URL filtering policies.
* Maintain, develop and enhance the capability and integration of endpoint security control applications.
* Review and contribute to the security incident response plan and accompanying playbooks.
* 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, and business unit to carry out tasks in support of CSIRO scientific objectives.
* Adhere to the spirit and practice of CSIRO’s Code of Conduct, Health, Safety and Environment plans and policies, Diversity initiatives and Zero Harm goals.
* Other duties as directed.

## **Selection Criteria**

#### Essential

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

* Minimum of five (5) years’ experience working in an ICT cyber security role within the large enterprise, system integrator or service provider space, **or similar role**, such as network/infrastructure/systems engineering.
* Demonstrated experience using, managing and tuning endpoint security solutions (e.g. EDRs/XDRs)
* Demonstrated experience using, managing and tuning a SIEM or similar platform (e.g. Splunk, Sentinel)
* Demonstrated ability to apply analytical, conceptual thinking and broad technical skills to detect, identify, investigate, and manage malicious activity and behaviour, intrusions, compromises, threats and anomalies
* Demonstrated experience with incident investigations and response or similar complex troubleshooting activities
* Demonstrated ability to collaborate widely both internally and externally and provide advice and recommendations

**Desirable:**

* Cyber Security related certifications (e.g. CCNA Cyber Ops, SSCP, CISSP, GSEC)
* Experience using, managing and tuning the security related features of next-generation firewall solutions (e.g. URL filtering, threat detections, logging, etc)
* Demonstrated experience using, managing and tuning SOAR or similar automation tools and techniques.
* Experience with the application of programming and/or scripting languages to assist in automation or service improvements (Bash, Python, PowerShell, etc)

## **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.

Special Requirements

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

Include if relevant:

* 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 NV1 security clearance level.
* Due to the nature of this role and security considerations, this position is open to Australian Citizens only.
* *If you have any queries regarding finalising the Duties and Key Result Areas or the Special Requirements for this position, please consult with In-business HR or the Talent Acquisition Team.*

## **About CSIRO**

We solve the greatest challenges through innovative science and technology. Visit [CSIRO Online](http://www.csiro.au/) for more information.

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

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