# Position Details

## Technical Services- CSOF6

|  |  |
| --- | --- |
| The following information is for applicants | |
| Advertised Job Title | Cyber Security Operations Manager |
| Job Reference | 72008 |
| Tenure | Indefinite  Full-time |
| Salary Range | AU$113,338 to AU$132,811 pa + up to 15.4% superannuation |
| Location(s) | North Ryde, NSW – Black Mountain, ACT – Clayton, VIC |
| Relocation Assistance | Will be provided to the successful candidate if required |
| Applications are open to | * Australian Citizens Only |
| Position reports to the | Chief Information Security Officer |
| Client Focus – Internal | 80% |
| Client Focus – External | 20% |
| Number of Direct Reports | 5 |
| Enquire about this job | Alfred Dera at [alfred.dera@csiro.au](mailto:alfred.dera@csiro.au) or phone +61 9290 8956 |
| 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](mailto:careers.online@csiro.au) or call 1300 984 220. |

### Role Overview

The Cyber Security Services (CSS) team operates within the Information Management & Technology (IMT) business unit focusing on ongoing security operations, cyber resilience, and data protection.

CSS is seeking an efficient and analytical individual to lead and manage the Cyber Security Operations team focusing on incident response, monitoring, and analytics. This person will need to be self-motivated, comfortable working under pressure in a confidential environment and able to manage competing priorities. The Cyber Security Operations manager will be highly competent in managing and improving the ongoing functions of a SOC (Security Operations Centre) including responding to one or more incidents ranging from simple to complex within a high stress but rewarding environment.

### The successful candidate will be expected to demonstrate effective leadership of the team. They will also contribute to the evolving technical capabilities within the team, undertake professional development supporting the ever-changing cyber environment and mentor other team members.

### Duties and Key Result Areas:

* Direct both the Monitoring & Analytics and Incident Response teams within CSS Operations.
* Drive and support the ongoing evolution of CSIRO’s, cyber threat detection and response capability including real-time monitoring and data analysis.
* Ensure effective response to security incidents through appropriate application of people, processes, and technology resources.
* Take ownership or delegation of potentially high-pressure security incidents involving inappropriate or malicious activity and behaviour, intrusions, compromises, threats, and anomalies on the network.
* Empower the Monitoring & Analytics and Incident Response team leaders through effective leadership, mentoring, decision making, organisational skills, and overall support to enable them to undertake effective performance management and career development of staff and optimise service efficiencies.
* Influence ongoing positive relationships with IMT management and staff to maintain optimal coverage, performance, and health of existing and new security ‘sensors’, controls, and countermeasures, processes, and effective resolution of issues.
* Support, contribute, and influence organisational wide cyber security deliverables including but not limited to risk reduction activities, capability enhancement, and security awareness programs.
* Liaise with vendors in the delivery of secure and reliable products and services through productive ongoing technical and commercial engagement while monitoring returns on investments.
* Liaise with government and law enforcement agencies with investigations, incidents, collection of evidence, and sharing of threat intelligence and advisories.
* Assume responsibility for all CSS operations security, strategic alignment, business, capacity planning, financial management activities and reporting mandates, especially in the ongoing quality improvements of relevant data driven security metrics reporting as per the ever-changing cyber threat environment.
* Lead an effective team, allocate and manage resources and undertake staff performance management and career development.
* 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, often regionally dispersed research team, and business unit to carry out tasks in support of CSIRO’s 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.

## **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.

## **Selection Criteria**

#### Essential

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

1. Formal tertiary qualifications in one or more of the following: Computer Science, Engineering, or related technical field. In lieu of this, a minimum of ten (10) years’ experience working in an ICT environment may be substituted.
2. At least two (2) years managing a cyber security team in an operational capacity or at least five (5) years managing an IT team.
3. Demonstrated experience with leading and application of monitoring, analysis, and management of security events and incidents using multiple sources and industry tools within a complex environment.
4. Demonstrated experience in applying leadership, analytical, conceptual thinking, and technical skills to detect, investigate, and manage malicious activity and behaviour, intrusions, compromises, threats, and anomalies on the network.
5. Demonstrated ability to collaborate widely both internally and externally and provide advice and recommendations to managers and staff.
6. Excellent written and verbal communication and reporting skills with a high level of literacy and editing skills.
7. Strong organisational, mental resilience, analytical and problem-solving skills.
8. Demonstrated ability to manage competing complex demands; establish or renegotiate priorities; organise or re-assign tasks and meet deadlines.
9. Ability to deal with incomplete information, ambiguity, urgency, and complexity when developing appropriate responses and strategies.

## **Desirable:**

1. A solid understanding of the wider industry security environment and experience working with various cyber security technologies.
2. Cyber Security related certifications (e.g. CISM, CISSP, SABSA)
3. Experience with the application or understanding of contemporary programming and/or scripting languages.
4. Experience with the application or understanding of complex network technologies.
5. Demonstrated experience working with Cyber Security industry tools including but not limited to Splunk, Carbon Black and Cylance.

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.

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

## **About CSIRO:**

We solve the greatest challenges through innovative science and technology. To find out more visit us [online](http://www.csiro.au/)!

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