# Position Details

## Technical Services- CSOF5

|  |  |
| --- | --- |
| The following information is for applicants | |
| Advertised Job Title | Senior Cyber Security Analyst |
| Job Reference | 73274 |
| Tenure | Specified Term of 3 years |
| Salary Range | AU$98,735 to AU$106,848 pa (pro-rata for part-time) + up to 15.4% superannuation |
| Location(s) | Canberra, ACT; Brisbane, QLD; Sydney, NSW; Melbourne, VIC; or 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 Manager |
| Client Focus – Internal | 80% |
| Client Focus – External | 20% |
| Number of Direct Reports | 0 |
| Enquire about this job | Alfred Dera via email at [alfred.dera@csiro.au](mailto:alfred.dera@csiro.au) or phone +61 9290 8956  Marianne Cologon via email at [marianne.cologon@csiro.au](mailto:marianne.cologon@csiro.au) or phone +61 2 6218 3573 |
| 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.

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

### Duties and Key Result Areas:

* Conduct real time monitoring, analysis and triage of security events and alerts from multiple sources including, but not limited to, events from the Security Information and Event Tools, Log files, firewalls and intrusion detection/prevention systems, endpoint detection and response, and endpoint protection.
* Apply analytical, conceptual thinking, and technical skills to detect, identify, investigate, and manage malicious activity and behaviour, intrusions, compromises, threats, and anomalies on the network.
* Escalate and triage security alerts to the relevant team within CSS and IMT where applicable.
* Support the response to security incidents.
* Monitor the health of security ‘sensors’, controls, and countermeasures through observation of overall performance, security risks and exposure, and effective resolution of issues.
* Liaise with vendors in the delivery of secure and reliable products and services through management of support tickets and productive engagement.
* Develop detection strategies including attack models, use cases, to assist in further tuning detection capabilities and prevent incidents from recurring.
* Mentor and assist junior staff members through knowledge transfer and guidance.
* Work within the broader IMT team to assist in identifying and managing vulnerabilities through implementation of appropriate security controls.
* Improve relevant work procedures to ensure repeatability and efficiency.
* Ability to prepare reports, dashboards and documentation to support risk-based, informed executive decisions.
* 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.*

1. Minimum of two (2) years’ experience working in a cyber security operational capacity including actioning and triaging security alerts relating to the broader ICT environment.
2. Demonstrated experience applying real time monitoring, analysis and triage of security events and alerts from multiple sources and industry tools.
3. Demonstrated experience developing detection strategies, including attack models and use cases, to assist in further tuning detection capabilities and prevent incidents from recurring.
4. Demonstrated ability to apply analytical, conceptual thinking, and technical skills to detect, identify, investigate, and manage malicious activity and behaviour, intrusions, compromises, threats, and anomalies on the network.
5. Experience with incident investigation and resolution in a complex ICT environment working with multiple technical specialists and domains.
6. Experience with the application and operation of two or more of the following technologies and their security requirements: Splunk, Endpoint Detection & Response, Endpoint Protection (Anti-Virus), Threat Analytics, Vulnerability Management platforms, Intrusion Detection or Prevention systems, Firewalls, Email Security, Network Security, Active Directory, and DNS Security.
7. Experience with Microsoft, Linux/Unix operating systems and virtualisation technologies (Microsoft/VMware or Open Source).

## **Desirable:**

1. A solid understanding of the wider industry security environment and contemporary security technologies.
2. Cyber Security related certifications (e.g. CCNA Cyber Ops, SSCP, CISSP, GSEC).
3. Experience with the application of contemporary programming and/or scripting languages to assist in automation or service improvements.
4. Demonstrated experience with using Splunk in a security operations context.

## **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 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:

* 1. People First
  2. Further Together
  3. Making it Real
  4. Trusted