



Solsoft Recruitment

Department of Industry, Science and Resources

- RFQ No: LH-07702 **APS6 Senior Cyber Threat Analyst** last date to apply Friday, 02 October 2026
- Contract start Saturday, 17 October 2026 to 12 months Plus two 12-month extension.
- Australian Citizen Must be able to obtain Baseline – ACT - Hybrid.

Send your responses to jobs@solsoft.com.au

About the organisation

The Department of Industry, Science and Resources (DISR) is a department of the Australian Government established on 1 July 2022. It is responsible for advising the government on matters of industry, science and resources, and delivering policies and programs in these areas. The department is also responsible for the publication of the government's "Critical Minerals Strategy 2023–2030".

Job Details:

Threat Detection Engineer develops and maintains the material required to detect threats and incidents across the SOC technology stack.

The Threat Detection Engineer (TDE) is responsible for the research, development, testing and maintenance of use case and detection rules. They are to co-ordinate with Cyber Defence Analysts in developing detection content for use in the SIEM, SOAR and EDR platforms.

As part of the detection engineering lifecycle the TDE is expected to work in an ITIL and Agile environment, developing process and engineering documentation. The TDE is also responsible for providing threat intelligence sharing to infrastructure and architecture teams in both Cloud and onpremise environments.

Key duties and responsibilities

This position is responsible for:

- Develop use cases based off threat models, system risks, vulnerabilities, intelligence, incident reports and industry frameworks
- Develop the detection rule syntax associated with use cases within the SIEM and EDR technologies
- Develop playbooks for alert validation by understanding the context in which the detection rule is designed
- Develop and maintain threat models using industry recognised methodologies such as STRIDE, ATT&CK and attack path analysis to identify detection opportunities and coverage gaps.



Solsoft Recruitment

- Assess emerging threats associated with Artificial Intelligence (AI) platforms, services and agents, and develop detection content to identify AI-related misuse, data leakage, prompt injection, model abuse and adversarial activity.
- Collaborate with architecture and engineering teams to ensure threat modelling outcomes are translated into effective monitoring, detection and response capabilities.
- Maintain the threat intelligence integrations across the SOC technology stack
- Conduct in-depth research and analysis for new detection content
- Collaborate with Cyber Defence Analysts for detection rule tuning
- Assist with threat model development to inform the detection engineering strategy
- Assist in the identification of content shortfalls across the detection engineering practice
- Assist with incident response at that direction of the incident manager
- Assist in the onboarding of new data sources to meet requirements of use cases
- Provide evaluation and feedback necessary for improving intelligence production and reporting
- Provide support to designated exercises, planning activities, and time sensitive operations

Responses to selection criteria

Criteria

The buyer has specified that each candidate must provide a one page pitch to address all criteria specified. This is equal to 5000 characters.

Essential criteria

1. Detection Engineering and SIEM Expertise - Demonstrated experience developing detection content across at least two enterprise SIEM platforms (e.g. Splunk, Microsoft Sentinel, QRadar, Elastic).
2. Threat Detection and Response Capability - Experience developing and implementing detections across SIEM, SOAR and EDR platforms, including incident response automation and playbook development
3. Threat Modelling and Threat Intelligence - Practical experience conducting threat modelling using recognised methodologies (e.g. STRIDE, PASTA, ATT&CK) and translating outcomes into detection and monitoring requirements, supported by a strong understanding of the cyber threat intelligence lifecycle
4. AI Security Monitoring - Experience identifying, assessing and developing monitoring controls for AI-related security risks, including enterprise AI platforms such as Microsoft Copilot or Azure AI
5. Cyber Security Operations Experience - Minimum five years' experience in cyber security operations, supported by strong organisational, communication and stakeholder engagement skills.



Solsoft Recruitment

YOUR RESPONSE

Please respond to the following	I am authorising Solsoft exclusively to submit my application. Job Name: APS6 Senior Cyber Threat Analyst RFQ NO: LH-07702 Date: <response> Authorisation Of applicant: Yes No	
Name	First Name Surname	<response>
	Gender	<response>
Your mobile number plus email address	<response>	
Home address	<response>	
Availability	<response>	
Rate including super ex-gst	\$ PAYG (Y/N)	
Citizenship Status	Australian	
Security Clearance	Clearance Level:	<response>
	CSID number	<response>
Referee 1	Name:	<response>
	Title:/ Organisation	
	Professionals' relationship to you:	
	Phone:/Mobile	
	Email:	
Referee 2	Name:	<response>
	Title:/ Organisation	
	Professional relationship to you:	
	Phone:/Mobile	
	Email:	



Solsoft Recruitment

• RESUME

Important: Softtestpays requires your CV as per below resume format

- SUMMARY

- TECHNICAL SKILLS

-

- EDUCATION

- TRAINING AND CERTIFICATIONS

- WORK HISTORY

- Referees



Solsoft Recruitment

HOW TO ADDRESS KEY SELECTION CRITERIA

The following provides a guide on how to address key selection criteria when applying for public service positions, and hence is particularly valuable to forward onto prospective candidates.

BACKGROUND RESEARCH

This guide has been prepared from information gathered from a wide variety of government sources.

THE PROCESS

Firstly, analyse the criteria, and look for the key issue(s). Once identified, ensure that you adequately address these issues. Each Key Selection Criteria is best addressed by the examples of demonstrated experience in various projects.

Finally, conclude your response by forecasting how you could perform the key issue in the future in this position. A paragraph will suffice.

SUCCESS

Provide a validating statement on your success and how you know you were successful. For example, offer feedback received from your manager or clients, state any cost and work efficiencies and/or quality assurance results. This is where you sell yourself.

SUGGESTED PAGE LAYOUT

- Retype the Criteria (bold or italic)
- Initial Premise(s)
- Supporting argument (attempting to prove your premise)
- Validating statement(s) (quote 3 or 4 examples – don't make them too long, keep to the point)
- Summary
- How you believe your past experience will allow you to perform in the future
- Only use "I" in your responses.

LENGTH OF RESPONSE

If your response is too long, you risk boring the readers and they will not read everything you have written.

Do not, under any circumstances, 'waffle on' about your accomplishments.

If you make it too short, then you run the risk of excluding information which may bias a selection decision and you may not score as highly as you should have.

Short paragraphs should be used, and length should depend on how much you have to say and the level of the position.

Ask yourself: Is this important to support my case on this criterion?



Solsoft Recruitment

Individual departments may provide a guideline as to the length of response they require – it is **critical** to the acceptance of your application that you adhere to guidelines provided which relate to response length.

Employ a strong positive approach demonstrating energy and initiative, but not arrogance. You should convey to the passive or neutral receiver that you should be interviewed. Always take into account the reader.

WHY GO TO THIS MUCH TROUBLE?

Addressing the selection criteria with quality responses demonstrates to the selection panel that you are not only qualified for the position, through your skills and experience, but that you are also committed to the role and have been prepared to take the time and effort to support your application.

Always bear in mind that the Selection Criteria process exists in the interests of equal and fair selection, based on merit, skills and experience.

SELECTION CRITERIA - MEANING OF TERMS

KNOWLEDGE

- 'Knowledge' – basic knowledge only is required. For example, you know which Act applied to a particular area and overall know what the Act covers.
- 'Sound Knowledge' – a good working knowledge. For example, you know policy provisions and intentions of an Act and the conditions under which benefits are conferred or obligations assumed.
- 'Thorough Knowledge' – highest level. You would be expected to know the details of an Act, the theory of an Act, etc.

ABILITY VS PROVEN ABILITY/DEMONSTRATED ABILITY

When the terminology 'ability to ...' occurs, it means that you need to provide specific examples of instances of where you have performed that function effectively.

In most cases, the list of duties will give you an idea as to the 'level' of 'knowledge' or 'ability' required to perform the duties.

Ensure that you relate your past performance and experience to every qualification and/or experience statement listed in the Selection Criteria.