Candidate Information Pack

Cyber Security Operations Analyst – Level 5-6

Position details

Title	Cyber Security Operations Analyst
Classification	Level 5 – Level 6
Location	Canberra
Salary Range	L5: $108,584 - $116,989 L6: $120,199 - $138,523
Contact	Recruitment Phone: (02) 6261 1849
Closing Date and Time	Monday 12th October 2026 at 23:59 AEDT

About ASIS

The Australian Secret Intelligence Service (ASIS) is Australia's overseas intelligence collection agency. We are Australia's experts at collecting highly sensitive information – secret intelligence – from sources overseas to keep Australia and our region safe and prosperous.

Our work spans continents and cultures. As a tech-powered and data-driven organisation, we use covert techniques and cutting-edge technology to put us in the right rooms, next to the right people, with the right access to the intelligence we need. We are tasked to collect intelligence – it might be political, military or economic information – deliberately withheld from the Australian Government that might present threats to or opportunities for Australia.

From graduates to career changers, we come from every corner of the country and all walks of life, with backgrounds from all around the world.

Regardless of our ethnicity, experiences and education, we're bound by a shared commitment to something bigger: building a better future for those who come after us. We seek to reflect the community we serve, and welcome applications from Aboriginal and Torres Strait Islander peoples, women, people with a disability, neurodiverse, people from culturally and linguistically diverse backgrounds and those who identify as LGBTQIA+.

It's a mission owned by everyone, with opportunities for all.

The role

Join us as a Cyber Security Operations Analyst and play a pivotal role in safeguarding ASIS's ICT environment. In this dynamic position, you will monitor, detect, and respond to malicious cyber activity, working to protect the confidentiality, integrity, and availability of our systems and sensitive data. From analysing log data through Security Information and Event Management (SIEM) platforms to conducting proactive threat hunting, your work will directly impact our ability to identify, contain, and eradicate threats to ASIS.

This role offers a unique blend of technical challenges and collaborative opportunities. You will leverage advanced technologies and data analysis to provide timely, actionable insights, develop dashboards and detection use cases, and work proactively to identify and remediate capability and coverage gaps across the ICT environment. You will also prepare for and manage cyber incident response activities, ensuring rapid and effective action when incidents occur.

As a key member of our team, you will have the opportunity to mentor and coach junior team members, sharing your expertise in best practices and contributing to their professional growth. We value candidates with a strong background in enterprise or government ICT environments, proficiency in cybersecurity tooling and SIEM platforms, and a solid understanding of virtualization and network fundamentals. Effective communication skills are essential, as you will interact with both technical and non-technical stakeholders. If you are passionate about cybersecurity, enjoy solving complex problems, and thrive in a collaborative environment, we invite you to apply and take your career to the next level with us.

Role responsibilities

- Monitor, detect, and respond to malicious cyber activity targeting ASIS's ICT environment to protect the confidentiality, integrity, and availability of systems and data
- Analyse log data from applications, hosts, and network traffic using SIEM software and conduct proactive cyber threat hunting activities
- Prepare for and manage cyber incident response activities, working to quickly identify, contain, and eradicate threats
- Develop dashboards, use cases, and threat detection capabilities to improve cyber security, and proactively identify and remediate capability and coverage gaps across the ICT environment
- Leverage advanced technologies, intelligence analysis, and data holdings to provide actionable insights and support other business areas
- Mentor and coach team members on cyber security operations best practices

Core skills

We encourage applicants with the following skills and attributes to apply:

- Familiarity with risk management, incident response, and investigative best practices, including experience in security analytics and developing reporting for various customers.
- Demonstrated understanding of Australian Government cyber security frameworks, including the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM).
- Strong background in cyber security capabilities and tools, including SIEM, data analytics platforms, and query/coding languages such as SQL, SPL, Python, and PowerShell.
- Demonstrated understanding of at least one technology domain, such as infrastructure, virtualisation, databases, software development, data analytics or machine learning.
- Proven ability to work under limited direction with reasonable autonomy, demonstrating initiative, judgment, and strategic thinking to solve complex problems and manage workflows.
- Excellent communication and stakeholder engagement skills, with the ability to provide detailed technical and policy advice, articulate cyber best practices, and manage sensitive issues.

Education and qualification requirements

The following education, qualifications and/or experience will be highly regarded:

- Proven experience in cyber security operations, including monitoring, detecting, and responding to malicious cyber activity
- Proficiency in Security Information and Event Management (SIEM) software, data analytics platforms, and query/coding languages (e.g., SPL, SQL, Python, PowerShell) is highly desirable
- Previous incident response experience, such as digital forensics, malware analysis and incident investigations will be highly valued
- Professional certifications along with demonstrated application of knowledge will be highly regarded
- Bachelor's degree in Cyber Security, Computer Science, or Information Technology (not essential)
- 3+ years of experience in a cyber-security operations or analyst role, preferably within an enterprise or government environment

Benefits of working at ASIS

ASIS employees enjoy access to generous workplace terms and conditions. Benefits include but are not limited to:

- Competitive salary plus 15.4% superannuation
- A variety of leave options including 22 days paid annual leave per year
- Paid leave between Christmas and New Year
- Domestic Relocation assistance for new staff to Canberra
- Health and wellbeing initiatives
- Salary packaging arrangements
- Learning and development opportunities including access to study assistance
- A variety of support services including but not limited to Employee Assistance Program (EAP) and a Staff and Family Support Office.

While ASIS officers are not able to work from home due to the classified nature of our work, staff have access to a range of flexible working arrangements. These include part time hours, condensed hours and/or flexible start/finish times to support other responsibilities.

ASIS conditions of service are similar to those applying for the Australian Public Service, for a full list of benefits and conditions see asis.gov.au

Eligibility

To be eligible for a role you must:

- Be an Australian citizen
- Be assessed as suitable to hold and maintain a TOP SECRET-Privileged Access security clearance
- For more information on eligibility please see the Protective Security Policy Framework which is publicly accessible at protectivesecurity.gov.au, section 12 provides information on Eligibility and suitability

How to apply

Click on "Apply Now" on our website on the role/s that you are applying for. You will be required to submit the following:

- 800-word pitch outlining your skills and experience for the role
- A current CV, no more than 2 pages in length, outlining your employment history, academic qualifications and relevant training that you may have undertaken
- Details of two referees, which must include a current supervisor

Applicants are encouraged to consider the Integrated Leadership System (ILS) capabilities when preparing their application. For more information on the ILS, and tips for applying for jobs in Australian Public Service, please visit the APSC website found at www.apsc.gov.au.

All applications for employment with ASIS are handled in the strictest confidence. It is essential you maintain a similar level of confidentiality and that you do not discuss your application with anyone.

Important:

If you are currently living overseas and wish to apply for a role with ASIS, please note that we cannot contact you until you return to Australia. Every part of the recruitment process, including contacting you, must be done while you are in Australia.

If you have no plans to return to Australia in the foreseeable future, we recommend you wait until you return before submitting an application.

Use of AI in recruitment process

We recognise some applicants may use AI technologies to draft applicants or prepare for interviews. If you wish to use AI, we recommend doing this only for initial drafts and ensure that your application is personalised and accurately reflects your skills, experiences and capabilities.

Additionally, be aware of the privacy policies of any AI tools you use. Be mindful of the information you are entering into AI tools (personal details, work history, etc) and how using it may link you to potential ASIS employment, noting that you are expected to maintain confidentiality with your application.

If you are invited to attend an interview, the use of AI tools and recording devices during the interview is strictly prohibited. Should AI tools or recording services be detected, your application, and any future applications may not be progressed.

Reasonable adjustments

ASIS is committed to fostering a diverse and inclusive environment for candidates to participate in all stages of the selection process. Please let us know if you require any additional assistance or reasonable adjustments during any stage of the recruitment process and we will work with you to manage this throughout. If you are successful in gaining employment, reasonable adjustments can also be made available to you in performing your role.

Recruitment process – what happens next

We thank all applicants for their interest in a role with ASIS. Please be advised that our selection process is rigorous and extensive and that we do not provide feedback to unsuccessful applicants. **If you progress from application, you will receive an SMS requesting you to complete online testing – please ensure that you complete this testing or your application will not progress further.**

All selection process decisions are merit based and candidates must be prepared to undergo various selection stages throughout the process.

A merit pool will be established for candidates who are suitable for this round and will remain valid for 18 months.