Candidate Information Pack

Cyber Security Operations Technical Lead – EL1

Position details

Title	Cyber Security Operations Technical Lead
Classification	EL1
Location	Canberra
Salary Range	$150,072 – $175,338
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 Technical Lead and play a pivotal role in safeguarding ASIS's global ICT environment. In this senior position, you will lead cyber incident response activities and technical investigations, driving efforts to quickly identify, contain, and eradicate threats to ASIS. From directing complex incident response operations to implementing detection engineering and intelligence capabilities, your work will directly shape our ability to protect the confidentiality, integrity, and availability of ASIS's systems and sensitive data.

This role offers a unique blend of technical leadership and strategic influence. You will lead the development of advanced detection capabilities while conducting proactive cyber threat hunting across the ICT environment. You will leverage advanced technologies and data analysis to provide timely, actionable insights, and proactively identify and remediate capability and coverage gaps to strengthen our security posture.

As a technical manager and key leader within our team, you will guide and mentor cyber security operations staff, fostering a culture of continuous improvement and excellence in tradecraft. You will coordinate with internal teams and stakeholders to drive operational priorities, uplift capabilities, and ensure the delivery of high-quality operational outcomes. We value candidates with extensive experience in cyber security operations, deep technical proficiency in SIEM platforms and analytics, and a proven track record of leading incident response and technical investigations. If you are passionate about cybersecurity, thrive in a fast-paced and collaborative environment, and are ready to take on a technical leadership role, we invite you to apply and make a meaningful contribution to ASIS's mission.

Role responsibilities

- Lead the monitoring, detection, and response to cyber activity impacting ASIS's ICT environment, ensuring the confidentiality, integrity, and availability of critical systems and data
- Lead technical investigations including analysis of security event logs, network traffic and system activity to identify, understand, respond and prevent cyber security incidents
- Drive the development and implementation of detection engineering and intelligence capabilities, designing advanced dashboards, use cases, and threat detection mechanisms to uplift ASIS’s cyber security
- Lead proactive cyber threat hunting activities using SIEM platforms, data analytics, and intelligence to proactively detect malicious activity on ASIS’s ICT systems
- Proactively identify capability and coverage gaps across the ICT environment, managing strategic remediation activities and leveraging data holdings to provide actionable insights and support complex investigations

- Provide technical leadership, mentorship, and coaching to cyber operations staff, managing workflows, setting operational priorities, and driving continuous improvement in tradecraft and incident response methodologies

Core skills

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

- Extensive experience in leading complex incident response, technical investigations, and risk management
- Applied understanding of Australian Government cyber security frameworks, including the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM), with the ability to translate these into technical security controls and operational strategies.
- Advanced expertise in cyber security capabilities and tooling, including architecting and optimizing SIEM platforms, leading detection engineering efforts, and leveraging query/coding languages (e.g., SQL, SPL, Python, PowerShell) to automate and enhance threat detection.
- Broad and deep technical knowledge across multiple technology domains (such as infrastructure, virtualisation, cloud, data analytics, or software development) to understand complex enterprise architectures and identify systemic threats.
- Proven technical leadership capabilities, demonstrating high-level judgment, strategic thinking, and the ability to work autonomously to solve complex problems, manage operational workflows, and uplift team capabilities.
- Exceptional communication and stakeholder engagement skills, with the ability to provide authoritative technical advice, brief senior stakeholders, articulate cyber best practices, and manage highly sensitive operational issues.

Education and qualification requirements

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

- Extensive experience leading cyber security operations, including the monitoring, detection, and response to sophisticated malicious cyber activity
- Advanced expertise in Security Information and Event Management (SIEM) software, data analytics platforms, and query/coding languages (e.g., SPL, SQL, Python, PowerShell) to drive detection engineering and automation
- Proven experience leading technical components of complex incident response activities, which might also include digital forensics or malware analysis.
- Professional certifications along with demonstrated application of knowledge are highly regarded

- Bachelor's degree in Cyber Security, Computer Science, or Information Technology (not essential)
- 5+ years of experience in a cyber security operations or analyst role, with demonstrated technical leadership experience 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.