Selection Documentation

Cyber Security

Executive Level 1

Salary: $145,137 - $169,572 (Plus Superannuation)

ASIS is Australia's overseas secret intelligence collection agency. Its mission is to protect and promote Australia's vital interests through the provision of intelligence services as directed by the Australian Government. Its work can involve collecting intelligence relating to national security, international relations and economic issues. It also contributes to Australia's coordinated national efforts against terrorism, proliferation of weapons of mass destruction, and trans-national issues such as people smuggling.

ASIS employs people in a wide range of roles, including technologists. These roles require dynamic team players who enjoy working with stakeholders, team members and individually on projects. ASIS is looking for people who will be able to meet tight deadlines and work to support ASIS priorities. Sucessful candidates will have excellent coordination and administration skills, excellent verbal and written communication skills; and, strong stakeholder engagement and influencing skills. Relevant tertiary qualifications and demonstrable experience will be highly regarded.

ASIS values workplace diversity and is committed to providing a supportive, inclusive and respectful work environment. We encourage applications from Aboriginal and Torres Strait Islander People, women, people with disabilities, people that identify as LGBTIQ+ and people from culturally and linguistically diverse backgrounds.

We offer a competitive salary package including 22 days annual leave, shutdown between Christmas and New Years Day, 15.4% employer superannuation contribution, and generous paid parental leave. Full and part time positions as well as flexible work hours can be negotiated.

All positions are office-based and located in Canberra. **This role requires the successful applicant to obtain and maintain a Security Clearance.**

ASIS is seeking to place enthusiastic and capable cyber specialists in a number of positions across the Service including lead roles in cyber security engineering, cyber security operations and cyber security assurance within a key Operational Technology area. In addition to our current vacancies, successful applicants through this process will be placed in a merit pool which may be utilised to fill future vacancies over the next 18 months. You will be asked to indicate your main area of interest/experience.

If you are interested in working in a particular area, we encourage you to tailor your responses to indicate your relevant skills and experience with regards to that function.

About the Teams

Operating within either the Security Branch or as a member of a key Operational Technology area, Cyber Security Directorate monitors, enables, and advises on the cyber security of the myriad technologies that underpin ASIS's business and operations. Cyber Security is multi-disciplinary team that consists of three key work streams – Operations, Engineering, and Assurance – that provide the following services:

1. Operations
    a. Develop, monitor, and triage security logs and alerts;
    b. Coordinate delivery of the Service's cyber security incident response activities; and
    c. Undertake threat hunts to proactively identify anomalous network activity.
2. Engineering
    a. Collaborate with key stakeholders to identify and address cyber security capability gaps;
    b. Plan and manage the development of current and future cyber security capabilities;
    c. Maintain cyber security capabilities as exemplars of effective and secure system design, in a high-security environment.
3. Assurance
    a. Assess and report on the cyber security risk posture of ASIS's systems;
    b. Provide security architecture advice to ASIS's projects and system managers; and
    c. Develop and deliver cyber security awareness campaigns to ASIS staff.

Please ensure you identify the specific role(s) you would like to be considered for when submitting your application.

Roles

Manager – Cyber Security Operations

You will develop, manage and lead the Operations team, responsible for the cyber security monitoring of ASIS's systems, and coordination of the Service's cyber incident response activities. You will manage the delivery of ASIS's cyber security incident response framework, encompassing activities from effective security monitoring (including user activity monitoring), through to remediation and recovery following a cyber security incident. You will guide the development of accurate and informative security reporting for customers, and continuously engage with industry and partners to identify improved ways of working.

To be successful in this role, you will have:

- Familiarity with risk management, incident response, and investigative best-practices.
- Demonstrated understanding of the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), and/or Essential Eight (E8) requirements.
- Demonstrated understanding of at least one technology domain (e.g. infrastructure, virtualisation, databases, software development, data analytics, machine learning, etc.).
- A proven ability to communicate complex issues to technical and non-technical audiences.

Technical Lead - Cyber Security Operations

You will perform a technical lead role either within the Operations team or as a member of a key Operational technology area. You will lead the delivery of robust, scalable, and fit-for-purpose cyber security use cases that support the detection of key threats to the Service. In the event of an incident, you will lead the delivery of Service's cyber security incident response activities. You will also identify and lead cyber security threat hunt activities to proactively identify potential threats to ASIS's systems.

To be successful in this role, you will have:

- Experience managing investigations, performing security analytics, and developing reporting for various (e.g. technical, non-technical, senior, and junior) stakeholder groups.
- Demonstrated understanding of at least three technology domains (e.g. infrastructure, virtualisation, databases, software development, data analytics, machine learning, etc.).
- Familiarisation with cyber security capabilities including SIEM and Data Analytics platforms, query/coding languages such as SQL, SPL, Java, Python and/or PowerShell, and digital forensics.

Technical Lead - Cyber Security Engineer

You will perform a technical lead role either within an Engineering team or as a member of a key Operational technology area. You will lead the development and maintence of technical capabilities that directly support the broader team's services. You will contribute to the execution of ASIS's Cyber Security Capability Roadmap by: researching, developing and integrating new technical capabilities to ensure coverage and collection of valuable audit events, optimising the sustainment of capabilities by automating routine tasks and processes, and ensuring the team's capabilities are exemplary high-security systems. You will build valuable working relationships across teams, vendors and partner agencies to ensure technical capabilities are implemented on-time and to-specification.

To be successful in this role you will have:

- Hands-on experience in delivering technical capabilities.
- Familiarisation with ICT Infrastructure and networking, data processing, SIEM platforms, vulnerability management, and cloud security (e.g. Azure and AWS).
- Proven ability to translate user requirements into technical features/functions.

Manager – Cyber Security Assurance

You will develop, manage and lead an Assurance team or as a lead in a key Operational techology area, responsible for cyber security assessment, architecture advice, and education within ASIS. You will manage the delivery of ASIS's security assessment and authorisation program, covering network penetration testing, vulnerability managment, and configuration analysis to report on and remediate identified vulnerabilities. To enable the implementation of secure systems, you will guide your team in the development of threat models and scenarios to validate security-enforcing controls, and recommend mitigations and countermeasures to address identified risks.

To be successful in this role, you will have:

- Familiarity with both risk management, and assessment/audit best-practices.
- Demonstrated understanding of the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), and/or Essential Eight (E8) requirements.
- Demonstrated understanding of at least one technology domain (e.g. infrastructure, virtualisation, databases, software development, data analytics, machine learning, etc.).
- Proven ability to communicate complex issues to technical and non-technical audiences.

Education, Qualification and Experience

For all roles, the following education, qualifications and/or experience will be highly regarded, though not essential:

- Experience in the management and/or development of a specialist team.
- Excellent coordination, administration, verbal and written communication skills.
- 5+ years of experience in a relevant field of expertise.
- Industry certifications including, but not limited to: Cert IV in Government Investigations, IRAP, CISA, CRISC, CCSP, CISM, CISSP, SABSA, OCSP, Microsoft, Linux, Cisco, Splunk.

Selection Criteria

Candidates are not required to provide a separate written response to the ILS capabilities (below), however, candidates are encouraged to consider the capabilities in preparing their application, as each candidate will be assessed on their ability to demonstrate behaviours aligned to the capabilities for the position.

For more information on the ILS, tips on applying for jobs in the Public Service, go to the APSC website found at www.apsc.gov.au.

Shapes Strategic Thinking

- Inspires a sense of shared purpose and direction;
- Focuses strategically;
- Harnesses information and opportunities; and
- Shows judgment, intelligence and common sense.

Achieves Results

- Builds organisational capability and responsiveness;
- Marshals professional expertise;
- Steers and implements change and deals with uncertainty; and
- Ensures closure and delivers on intended results

Cultivates Productive Working Relationships

- Nurtures internal and external relationships;
- Facilitates cooperation and partnerships;
- Values individual differences and diversity; and
- Guides, mentors and develops people.

Exemplifies Personal Drive and Integrity

- Demonstrates public service professionalism and probity;
- Engages with risk and shows personal courage;
- Commits to action;
- Displays resilience; and
- Demonstrates self-awareness and a commitment to personal development.

Communicates with Influence

- Communicates clearly;
- Listens, understands and adapts to audience; and
- Negotiates persuasively.

Job Specific Requirements

- Demonstrated experience and education relevant to the role.

HOW TO APPLY

Applicants will need to apply **ONLINE** via our website.

Applicants will required to attach a resume and submit a maximum 800 word pitch outlining their relevant experience, skills and knowledge to perform the duties of the role.

Applicants are encouraged to consider the capabilities when preparing their application, as this will form the basis of selection assessment. For more information and tips on applying for jobs in the Public Service, search 'Joining the APS' at www.apsc.gov.au.

After application submission, you may receive an SMS requesting you to complete online testing. Please ensure you complete this as your application will not be progressed otherwise.

APPLICATIONS CLOSE: Refer to date on website

ELIGIBILITY

Candidates must be Australian citizens.

The successful candidate will be required to obtain and maintain a security clearance.

REASONABLE ADJUSTMENTS

All requests for reasonable adjustments will be considered and managed in consultation with you. We will continue to ask you if you require reasonable adjustments at each stage of the process. If you are successful in gaining employment, reasonable adjustments can also be made available to you in performing your role.

WHAT HAPPENS NEXT?

You may receive a SMS requesting you to complete online testing. Please ensure you complete this as your application will not be progressed otherwise.

Please do not tell anyone about your application with our organisation at this stage of the process as doing so may harm your suitability for employment with us.

A merit list will be established for candidates who are suitable and will remain valid for a period of 18 months.

We thank you for the time and effort you have put into your application; however, we are unfortunately unable to provide feedback to unsuccessful candidates.