Selection Documentation

Cyber Security Specialist

Level 5-6

$105,013 - $133,968 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 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, administration and technical 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 is a diverse and inclusive workplace, where our people are empowered through authenticity and a sense of belonging to achieve their potential and contribute to a shared purpose and mission. 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 LGBTIQA+.

We offer a competitive salary package including 22 days annual leave, shutdown between Christmas and New Years Day, 15% employer superannuation contribution and generous paid maternity/paternity leave. Full and part time positions as well as flexible work hours can be negotiated.

These roles are **Canberra office-based** with successful applicant required to **obtain and maintain a Security Clearance.**

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. (Operations, Engineering, Assurance)

ROLE: Cyber Security Specialist (Level 5-6)

Operating within Security Branch, 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

Analyst – Cyber Security Operations

You will be a member of 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 support the delivery and day-to-day use of cyber security use cases, to enable the detection of key threats to the Service. In the event of an incident, you will support the delivery of Service's cyber security incident response activities. You will also support cyber security threat hunt activities to proactively identify potential threats to ASIS's systems.

To be successful in this role, you will have:

- Familiarity with risk management.
- A working understanding of the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), and Essential Eight (E8).
- Experience within at least one technology domain (e.g. infrastructure, virtualisation, databases, software development, data analytics, machine learning, etc.).
- A desire to refine and expand your technical knowledge and skills in a cyber security context, including, but not limited to: SIEM and Data Analytics platforms, query/coding languages such as SQL, SPL, Java, Python and/or PowerShell, and digital forensics.

Engineer - Cyber Security Engineer

You will be a member of the Engineering team. You will support 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 supporting the secure management of the team's capabilities.

To be successful in this role you will have:

- Familiarity with risk management.
- A working understanding of the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), and Essential Eight (E8).
- Experience within at least one technology domain (e.g. infrastructure, virtualisation, databases, software development, data analytics, machine learning, etc.).
- A desire to refine and expand your technical knowledge and skills in a cyber security context, including, but not limited to: infrastructure and networking, data processing, SIEM platforms, vulnerability management, cloud security (e.g. Azure and AWS), project management, and business requirements modelling.

Assessor – Cyber Security Assurance

You will be a member of the Assurance team, responsible for cyber security assessment, architecture advice, and education within ASIS. You will support the delivery of security assessments against ASIS's systems, 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 develop 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 risk management.
- A working understanding of the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), and Essential Eight (E8).
- Experience within at least one technology domain (e.g. infrastructure, virtualisation, databases, software development, data analytics, machine learning, etc.).
- A desire to refine and expand your technical knowledge and skills in a cyber security context, including, but not limited to: vulnerability management tools, penetration testing tools and techniques, Governance, Risk and Compliance (GRC) tools and processes, etc.

Education, qualification and experience requirements

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

- Relevant tertiary qualifications or experience in Cyber Security, IT, Systems Engineering or a related field;
- Experience with open source / COTS / GOTS cyber security tools;
- Demonstrated experience working in Cyber Security or ICT-related areas

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.

Supports Strategic Direction

- Supports shared purpose and direction;
- Thinks strategically;
- Harnesses information and opportunities; and
- Shows judgment, intelligence and common sense.

Achieves Results

- Identifies and uses resources wisely;
- Applies and builds professional expertise;
- Responds positively to change; and
- Takes responsibility for managing work projects to achieve results.

Supports Productive Working Relationships

- Nurtures internal and external relationships;
- Listens to, understands and recognises the needs of others;
- Values individual differences and diversity; and
- Shares learning and supports others.

Displays Personal Drive and Integrity

- Demonstrates public service professionalism and probity;
- Engages with risk and shows personal courage;
- Commits to action;
- Promotes and adopts a positive and balanced approach to work; and
- Demonstrates self-awareness and a commitment to personal development.

Communicates with Influence

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

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.
