



APS Level 4-5 - Security Analyst

Job Reference Number: JCG/12510/23

Salary: \$73,343 - \$86,211 (plus Super and 15% BDCP)

Position Location: Harman - ACT

Employment Status: Ongoing - Actual vacancy - Full time (37.5 hours per week)

Security Level: Positive Vetting

Group: Joint Capabilities Group

Division: ICT Operations Division

Contact Officer: Kacie Eaton
02 5131 3185
Kacie.Eaton@defence.gov.au

Closing Date: 11:30pm (AEDT), Wednesday 24 January 2024
Extensions may be granted in exceptional circumstances only.



Your Role

As an effective Security Analyst within the Sensitive Data Analysis Team you will have the opportunity to:

- Engage with stakeholders, under direction, identifying and responding to needs and expectations. Utilise or acquire digital forensics skills by contributing to investigations through processing and analysing artefacts in line with evidentiary process, policy, standards and guidelines to support production of forensics findings and reports.
- Analyse data artefacts, exercising initiative and judgement in line with policy, standards and guidelines to identify breaches of policy, regulation or law. Support the preparation of reports to communicate insights drawn from analysis of a range of data sources.
- Assess the integrity of data to provide advice on the transformation of data from one format/medium to another while maintaining and implementing information handling procedures.
- Enable the availability, integrity and traceability of information through the application of formal data and metadata structures and protection measures.

The additional payment is a Building Defence Capability Payment (BDCP) which enables Defence to provide a premium, in addition to the rate of salary otherwise payable under the Enterprise Agreement (EA) to some or all of the jobs within a critical occupation(s) or discipline within a workplace. Applicants engaged into a BDCP position must consider the following. BDCPs provide remuneration in addition to the Defence Enterprise Agreement (EA). This arrangement is subject to meeting eligibility criteria and is subject to annual review. Should your performance fall beyond requirements or the eligibility criteria not be met, your eligibility for the BDCP may be reviewed and ceased. It may also be ceased should you change positions or the requirement for the BDCP is no longer necessary, as determined by Defence. Should the BDCP be ceased you will be advised and your BDCP additional payment will cease.

Our Ideal Candidate

You will have or be able to rapidly obtain data analysis skills and/or experience, including the ability to understand and interpret technical data from a variety of sources, including structured and unstructured datasets to respond to requests for information and incident response requirements in a timely manner.

The following attributes, skills and experience will be highly regarded:

- Understanding of investigative requirements, including evidentiary data handling, interpretation, analysis and identification. High attention to detail regarding data manipulation and analytical skills.
- Ability to interpret and convey technical information to a broad range of stakeholders. Stakeholder engagement and time management skills with a focus on competing priorities.
- Experience with ICT analytical or forensic tools (e.g. x-Ways, NUIX/Ringtail, Axiom, FTK or similar).
- Experience in ICT incident response or investigations. Awareness of data security and classification handling requirements.

Our Organisation

Defence's primary mission is to protect Australia and its national interests, promote security and stability in the world, and support the Australian community as directed by the Government.

Defence Australian Public Service (APS) employees are engaged in an array of occupations, across Australia and around the world, enabling our three services: Navy, Army and Air Force, to fulfil key defensive roles as well as providing a range of peacetime services.

In Defence, you will enjoy experiences and opportunities that, as an APS employee, you simply would not get in any other organisation. You are able to undertake interesting, challenging and unique work. This ranges from intelligence and strategic policy right through to human resources, communications, infrastructure and engineering, and information technology.

Defence is committed to recruiting the right people, in the right jobs, at the right time - whether it is creating, acquiring or delivering Defence capability. Our greatest asset is our people.

A more diverse workforce supported by an inclusive culture enhances Defence's capability and effectiveness, as it draws on different ideas to innovate and adapt to a rapidly evolving strategic environment and the changing nature of warfare.

Our [Values and Behaviours](#) reflect the traditions and identities of the Australian Defence Force (ADF) and the APS. The values underpin Defence's corporate culture and contribute to achieving organisational goals.

Defence accommodates requests for reasonable adjustment for people with disability to assist in the application process and if successful, the inherent requirements of the position. Please inform the contact person listed on the front of this Information Pack should you require adjustments to be put in place. The [RecruitAbility](#) process applies to this role.

Defence's commitment to Indigenous Reconciliation, Aboriginal and Torres Strait Islander communities, and the whole-of-Government *Closing the Gap* strategy is outlined in [Defence's Reconciliation Action Plan 2019-2022](#).

Defence provides relocation assistance to eligible APS employees required to relocate. The level of assistance will vary depending on the reason for relocating and your personal circumstances. For more information, please [download the APS Relocation Assistance Handbook](#).

Our Group

Joint Capabilities Group (JCG) is a diverse group and is the lead accountability for the Space and Cyber Domains, and delivering other key enabling effects such as integrated logistics. JCG is instrumental in ensuring ADF warfighting effectiveness and supporting the delivery of Government directed outcomes. The work in JCG is fast paced, exciting and directly supports Defence's mission to defend Australia and its National Interests.

JCG consists of the Joint Logistics Command, Defence Space Command, Defence SIGINT and Cyber Command, Joint Capabilities Division, Cyber Warfare Division, the Australian Civil-Military Centre, Military Strategic Effects Branch, and the Information, Communications and Technology Operations Division.

Our Team

The Directorate of Insider Threat and Investigative Support (ITIS) is a highly skilled team comprised of cyber security professionals with a specialised focus on the timely detection and response to insider threats and digital indicators of security concern within the Defence Enterprise portfolio. ITIS is a multidisciplinary area operating within Defence's complex and high-tempo environment that works closely with internal and external stakeholders, including Investigative Authorities, to provide intelligence and digital artefacts to an evidentiary standard in support of investigations and security operations. The Sensitive Data Analysis Team undertakes specialist discovery and analysis of digital artefacts in support of Requests for Information (RFI) pertaining to Task Forces, Inquiries, external agencies and legal teams. This includes performing data traceability, bespoke digital forensics and incident response activities for niche datasets and systems.

Our Work Environment

As the range and nature of work in Defence is so diverse, so are the different work environments that our employees are located in.

The workplace environment requirements for this role include:

- Computer Use
- Generic screen based
- Graphical/Analytical based
- Sitting at desk

The role requires the occupant to work within a high-security and enclosed environment. Occasional travel to other work sites is required. Duties primarily relate to screen-based computer work.

Office Arrangement

Defence is committed to assisting its employees with flexible office arrangements. This position offers an On Site Office Arrangement.

Desirable Qualifications, Experience or Training

Certificate IV in Government Investigations (PSP40416) or the ability to obtain within 12 months from commencement of employment.

The following qualifications are highly desirable:

- SANS SEC401: Security Essentials.
- GIAC Battlefield Forensics and Acquisition (GBFA).

Experience in the following disciplines is highly desirable:

- Insider Threat.
- Intelligence.
- Data Analytics.
- Security Operations.
- Investigations.
- Digital Forensics.
- eDiscovery.

How To Apply

Apply for this role by submitting your application through our [online recruitment system \(eRecruit\)](#) located at Defence APS Careers. If you have any questions regarding this role, email the contact officer.

For more information please refer to the [Applicant User Guide](#). Further advice on addressing selection criteria can be found in '[Cracking the Code](#)' publication located on the Australian Public Service Commission website.

Vacancies will be extended **in exceptional circumstances only**. Applicants requesting an extension must contact the Contact Officer **24 hours prior** to the vacancy closing date.

Assessment Criteria

In your application you should provide a copy of your current Resume/CV and address the following:

An explanation of how your skills, knowledge and experience will be relevant to this role (limit your total response to 600 words).

PLEASE NOTE: Defence APS Careers is for job seekers only. We do not accept unsolicited resumes or applications from recruitment agencies and/or search firms and will not pay fees to any such organisations unless arranged with the provider prior to advertising the vacancy.

Eligibility

Employment with the Department of Defence is subject to conditions prescribed within the Public Service Act 1999.

Citizenship – To be eligible for employment with Defence, applicants must be an Australian citizen. Only in exceptional circumstances can this requirement be waived.

Health Assessment – As a condition of engagement, a mandatory pre-employment health assessment may be required where there are physical or medical requirements for the role. Your contact officer can provide further guidance on whether this is required for your role.

Security Clearance – The Australian community requires the highest level of integrity from Defence employees. The preferred applicant will be required to successfully undergo the [security clearance](#) vetting process at a specified clearance level.

Further information can be provided in the [Australian Government Security Clearance Applicant Guide Book](#). Please ensure that you read this information thoroughly and confirm that you meet the minimum requirements to be eligible to hold a security clearance at the required level. Please ensure that you are able to provide the necessary documents if you apply for the position. The security clearance level required for this position can be found on the front page of this Information Pack.

More information on the security clearance vetting process is available on the [AGSVA website](#).

Thank you for your interest
Department of Defence