GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

POSITION DESCRIPTION

Computer Network Defence (CND) Application Engineer L2

Unit/Branch, Directorate: Cyber Security Operations (CSO)
Information Assurance and Cyber Security Directorate

Location: Wellington

Salary range: H $79,797 - $119,695

Purpose of position:
The Computer Network Defence (CND) Application Engineer is responsible for the development and implementation of software solutions to support networks and capabilities used for Computer Network Defence operations and investigations. These engineering solutions are used to maintain and enhance the Cyber Security Operations units' ability to detect, discover, analyse and report sophisticated computer network exploitation and associated tools.

The Level 2 CND Application Engineer has significant experience in Software Engineering and will be specialising in the specific intricacies of engineering solutions for network defence – a unique skill set.

Our mission at the GCSB is to protect and enhance New Zealand's security and wellbeing

Our values are Respect, Commitment, Integrity and Courage

Information Assurance and Cyber Security Directorate purpose: The IAC Directorate contributes to the national security of New Zealand by providing technical advice and assistance to Government and organisations with significant national information infrastructures to enable them to protect their information from advanced technology-borne threats. To achieve this, the Directorate provides technical security inspections; high-grade encryption services; information assurance policy and advice; regulation of telecommunications & space activities; and high-end cyber security services to detect and respond to such threats.

Key accountabilities	Deliverables/Outcomes
Solution design and implementation • Research and develop new and innovative techniques to enable and enhance the National Cyber Security Centre's (NCSCs) discovery and detection of malicious network traffic • Engineer and integrate software solutions that enable efficient analysis and reporting of threats • Ensure that solutions are created, where possible, by leveraging existing partner community solutions	• Electronic attack threats to monitored entities' infrastructure are identified and understood • Technical analysis of detected threats identifies the capability and intention of the malware targeting the victim • Solutions and enhancements of CND capability are compatible with and extended to international partners for integration into their CND capabilities • Relevant partner developed CND software solutions are applied to GCSB CND systems to enhance existing capability
Maintain engineered solutions • Maintain engineered solutions • Produce, and make available, documentation on engineered solutions to ensure their longevity • Train CND specialists and relevant NCSC staff on the appropriate and efficient use of new CND tools • Ensure solutions and GCSB CND infrastructure are optimised through engagement with Systems Engineering	• Existing electronic attack detection systems remain operational and capable of detecting electronic attack • Detection capabilities are routinely investigated and ensured they are fit for purpose • Usable documentation is produced that clearly articulates the purpose and use of GCSB or partner engineered solutions to CND problems • Documentation is in line with any GCSB corporate standards, policies and guidelines • GCSB or partner (either internal or external) users are enabled to understand and use engineered solutions
Customer and partner engagement • Interact with partner CND Developers and Engineers • Actively participate in international partner threat and CND forums, analyst meetings and conferences • Collaborate with partner agencies, and contribute solutions to the international partner Cyber community and other relevant forums • Provide engineering or technical assistance to other NCSC and GCSB colleagues to enable the enhancement of business and process • Maintain a situational awareness of current items of CND interest	• The technical capability of individuals within the NCSC is valued at the national and international partner Cyber community level • The Systems Administrator maintains a high awareness of current CND issues and technological trends • Productive and enduring relationships are formed with domestic and international partners, and GCSB is noted as a valued partner within the international Cyber community

Contribute to the execution of the IACD Strategic Plan • Promoting cross-team collaboration through the execution of the IACD Strategic Plan and support for operational exchanges between different IACD business units • Participating in both functional (specific skill-sets) and cross-functional (mixed skill-sets) IACD teams at the request of the IACD Executive and Leadership group • Pro-actively demonstrating a willingness to transfer skill sets to other teams in times of operational surge and crisis • Making a constructive contribution to the execution of the Strategic Plan	• Team silos are visibly reduced and the focus of staff shifts from their own unit plan to delivering Directorate-wide objectives • Customer feedback suggests that the plan is having a positive effect on IACD's performance through the creation of a more obviously joined-up operating model • Policy and process gaps, which negatively affect IACD operations, are highlighted and rectified • Staff retain an active interest in developments within IACD beyond their normal area of operation
Health and safety (for self) • Work safely and take responsibility for keeping self and colleagues free from harm • Report all incidents and hazards promptly • Know what to do in the event of an emergency • Cooperate in implementing return to work plans • Be a **visible** role model at all times • **Follow** GCSB's safety rules and procedures	• A safe and healthy workplace for all people using our sites as a place of work • All requirements in the NZIC Health and Safety policy and procedures are met
Other duties	Any other duties that fall within the scope of the position

Position delegation	
Financial delegation:	None

Key stakeholders	
Internal:	• Information Assurance and Cyber Security staff • GCSB IT security staff • Other GCSB Staff as necessary
External:	• NZ Government Agencies • 2nd Party cryptologic agencies • Other national or international CND engineers • IT service providers

Person Specification	
Experience:	• Significant experience in software engineering using Python, Java, C, C++ or similar. The incumbent must have a minimum of 6 years' experience in software engineering. Ideally with a minimum of 2 years dealing with CND intricacies. • Desirable experience in IT security, computer forensics, or network defence • In-depth experience with forensic tools, processes and artefacts • Experience with operating systems, both UNIX / Linux and Windows • Experience with network defence and attack tools • Experience engineering scalable solutions that can process large datasets is desirable • Experience with querying, maintaining and manipulating SQL databases or distributed databases is desirable • Experience in creating user interfaces is desirable • Experience in engineering statistical analysis solutions is desirable
Knowledge and Skills:	• Knowledge of computer and network security, and computer network defence, gained through a mixture of commercial and/or GCSB Computer Network Defence experience totalling a minimum of 5 years • Excellent communication and interpersonal skills • Excellent organisational skills and the ability to prioritise and work to deadlines • The resilience to operate under pressure and correctly identify and assess risk, and make justifiable operational decisions
Qualifications and Courses:	• Tertiary degree, or equivalent experience, in Computer Science, Computer Forensics, Software Engineering, or Computer Security • Professional computing/networking qualification e.g. in computer networking, or systems administration is desirable • Professional Information Security certifications is desirable
Specific Job Requirements:	• Ability to obtain and maintain a TSS security

	clearance

NZIC Competencies

In addition to the Person Specification above, competency standards which outline the development requirements of the position are set out under the NZ Intelligence Community (NZIC) Career Pathways framework. The Career Pathways framework enables progression within the job.

Full descriptions of progression competencies and an overview of the NZIC Career Pathways framework is available on appointment.

The position is aligned to the Information Engineering competency framework.

Diversity and Inclusion

The GCSB recognises that our success requires us to have a workforce that reflects the community we serve and diversity in its widest context – where all people, regardless of difference are valued and respected.

One way we show our inclusion of those with diverse sexual and gender identifies is with a Rainbow Tick accreditation which we proudly received in 2019.

We are committed to building a workplace where we can say we have achieved – ***He waka eke noa*** – a canoe which we are all in with no exception.

Changes to Position Description

Positions in the GCSB may change over time as the organisation develops. Therefore we are committed to maintaining a flexible organisation structure that best enables us to meet changing market and customer needs. Responsibilities for this position may change over time as the job evolves. This Position Description may be reviewed as part of planning for the annual performance cycle.

Date PD reviewed: 10/09/2019

Signatures		
Manager's Name		
Signature		Date:

Employee's Name		
Signature		Date: