GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

POSITION DESCRIPTION

Computer Network Defence (CND) Systems Engineer (L2)

Unit/Branch, Directorate:	Cyber Security Operations (CSO) Information Assurance & Cyber Security Directorate (IACD)
Location:	Wellington
Reporting to:	Team Lead, Systems Engineering, Cyber Security Operations
Direct reports:	Nil
Salary range:	H $79,797 - $119,695

Purpose of position:
The CND Systems Engineer (Level 2) is responsible for the development, implementation and maintenance of technical IT solutions to support and enhance our Computer Network Defence (CND) capabilities. Our CND Systems Engineers combine their skills, knowledge and passion to design and build solutions, which further enhance our ability to detect, discover, analyse and report sophisticated threats to the security of New Zealand's most significant information assets

---

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, innovative solutions to enable and enhance NCSC's discovery and detection of malicious network traffic • Following good industry design practices to ensure that solutions meet highest standards in operations • Integration of hardware and software solutions that enable efficient analysis and reporting of threats • Working to automate development and deployment of technical solutions where possible and sensible • Working with other teams to ensure the successful and efficient implementation of new or enhanced capabilities	• 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 are designed to be inherently secure, resilient and scalable
Maintain engineered solutions • Continual review and improvement of engineered solutions and accesses • Effective testing and remediation of identified bugs and errors • Produce, and make available, documentation on engineered solutions to ensure their longevity • Pro-active maintenance, monitoring, alerting and support of various systems to ensure maximum performance, stability and uptime • Train CND specialists and relevant NCSC staff on the appropriate and efficient use of new CND tools • Providing support to the users of both CLASSIFIED and UNCLASSIFIED CND and other NCSC/IACD systems as directed • Adherence to industry standard practices for change and capacity management	• Existing detection systems remain operational and capable of detecting cyber threats • Detection capabilities are routinely reviewed to ensure they are fit for purpose • NCSC systems are proactively maintained to ensure they are available and responsive for users to fulfil their required functions • Usable documentation is produced that clearly articulates the purpose and use of GCSB or partner engineered solution to CND problems • Documentation is in line with any GCSB engineering standards, policies and guidelines • Users are enabled to effectively and efficiently use engineered solutions in support of their mission
Customer and partner engagement • Interact with partner Developers and Engineers • Actively participate in community and industry forums, meetings and conferences • Provide engineering or technical assistance to other NCSC and GCSB colleagues to enable the enhancement of business and process • Maintain an awareness of information	• The technical capability of individuals within the NCSC is valued at the national and partner community level • The CND engineer 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 community

security and general IT industry trends and developments	
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:	• Three to five years' experience of Linux and/or Windows system administration • Experience with automation, configuration management and monitoring tools • Experience with network engineering or administration • Experience with system architecture, design and implementation of server and desktop systems • Experience and knowledge of IT operations models and Service Management processes (such as Change Management, Incident Management, Configuration Management and SDLC)
Knowledge and Skills:	• The ability to use or learn about a wide variety of Open Source technologies • Demonstrates a practical and robust troubleshooting philosophy • A commitment to the documentation of process and actions • Results oriented with a demonstrable commitment to perform • Thinks critically and logically • Excellent communication and interpersonal skills • The ability to be self-motivated, flexible and a team player • An ability and desire to learn new and sometimes complex skills
Qualifications and Courses:	• Tertiary degree, or equivalent experience, in Computer Science, Network Engineering, Systems Engineering or Computer Security • Professional computing/networking qualification, e.g. in computer networking, or systems administration is desirable • Professional Information Security certifications is desirable • DevOps and/or IT Service Management and Governance frameworks 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: