GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

# POSITION DESCRIPTION

## Computer Network Defence (CND) Analyst

| | |
|---|---|
| **Unit/Branch, Directorate:** | **Cyber Security Operations, Information, Assurance and Cyber Security Directorate** |
| **Location:** | Wellington |
| **Reporting to:** | Team Lead, Intrusion, Detection and Discovery |

---

**Purpose of position:** The Computer Network Defence (CND) Analyst seeks to discover, analyse and report on sophisticated computer network exploitation events. The CND Analyst utilises open source, commercial and internally developed intrusion/anomaly detection tools and infrastructure.

---

**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 |
|---|---|
| **Understanding the Cyber Threat Environment**<br>• Maintain an understanding of threat actor tactics, techniques and procedures (TTPs)<br>• Maintain an understanding of attack tool capabilities and infrastructure<br>• Conduct technology-based research projects, incorporating classified and open source material to maintain subject matter expertise in relevant CND topics<br>• Based on understanding the Cyber Threat Environment develop new analytic techniques to identify threats to New Zealand | • GCSB remains aware of cyber threat actors' intentions and capabilities and is postured to identify these<br>• NCSC (National Cyber Security Centre) is recognised as the foremost expert on Cyber security within New Zealand Government |
| **Conduct CND Activities**<br>• Contribute to the discovery and analysis of new or emerging cyber threats<br>• Prepare, document, and maintain analytic reporting<br>• Contribute to the detection, analysis and understanding of sophisticated electronic attack events<br>• If required, assist with the analysis of forensic evidence, in support of the Incident Coordination and Response Team<br>• Develop, maintain, and improve technical understanding and analytic techniques relevant to the role<br>• Share knowledge of these analytic techniques to NCSC colleagues, as appropriate | • Threats to New Zealand information infrastructures of significance are identified and understood<br>• Analysis is performed in accordance with agreed procedures<br>• NCSC's detection capabilities are enhanced |
| **Delivery of Output**<br>• Provide technical advice regarding the compromise of New Zealand victim networks. Contribute to mitigation design, and advice<br>• Enhance GCSB's relationships and reputation with customers and partners through professional representation and engagement<br>• Represent GCSB as a knowledgeable point of contact for information regarding specific high-threat intrusion set(s)<br>• Provide technical assistance to other NCSC, partner or customer entities | • NCSC provides timely and accurate technical advice and expertise<br>• The content of the NCSC's technical reporting and advice is unambiguous, and the implications of why it has been provided are clear<br>• The result of technical analysis is documented<br>• NCSC reporting complies with all guidelines and policies |
| **Health and Safety (for self)** | |

| | |
|---|---|
| • Work safely and take responsibility for keeping self and colleagues free from harm<br>• Report all incidents and hazards promptly<br>• Know what to do in the event of an emergency<br>• Cooperate in implementing return to work plans<br>• Be a **visible** role model at all times<br>• **Follow** GCSB's safety rules and procedures | • A safe and healthy workplace for all people using our sites as a place of work<br>• 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: | • Other NCSC and GCSB Team members |
| External: | • NCSC Customers<br>• Domestic and International Partners |

| **Person Specification** | |
|---|---|
| Experience: | • Experience in IT security or network defence or penetration testing.<br>• Knowledge of common network defence and attack tools and techniques<br>• Experience with operating systems, both UNIX / Linux and Windows<br>• Experience with programming / scripting |
| Knowledge and Skills: | • Interest in, and enthusiasm for, computer security<br>• A desire to work in a highly collaborative team environment<br>• Excellent knowledge of network protocols or host internals<br>• Software engineering and programming<br>• Knowledge of vulnerability assessment methodologies, tools and techniques<br>• Demonstrates a practical and robust troubleshooting philosophy<br>• A commitment to the documentation of |

| | |
|---|---|
| | process and actions<br>• Results orientated with a demonstrable commitment to perform<br>• Thinks critically and logically<br>• Excellent communication and interpersonal skills<br>• The ability to be self-motivated, flexible and a team player<br>• An ability and desire to learn new and sometimes complex skills<br>• Demonstrate sound judgment, tact and integrity in dealing with sensitive issues<br>• Excellent organisational skills and the ability to prioritise and work to deadlines<br>• Displays initiative and self-confidence<br>• The resilience to operate under pressure and correct 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<br>• Professional computing/networking qualification, e.g. in computer networking, or systems administration is desirable<br>• Professional Information Security certifications are desirable |
| Specialist Competencies<br>*These would typically be expected for the 100% fully effective level* | • Network and Endpoint Intrusion Detection, Methods and Signature Development<br>• Network Protocol Analysis<br>• Malware Analysis and Reverse Engineering<br>• Adversary Intentions and Methodology<br>• Programming / scripting |
| 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.

GOVERNMENT COMMUNICATIONS SECURITY BUREAU

BEYOND ORDINARY
We are. **Are you?**

## 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: 9/01/2019

| **Signatures** | | |
|---|---|---|
| Manager's Name | | |
| Signature | | Date: |

| | | |
|---|---|---|
| Employee's Name | | |
| Signature | | Date: |