GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

POSITION DESCRIPTION

Cyber Incident Responder

Unit/Branch, Directorate:	**Incident Coordination and Response** **National Cyber Security Centre** **Information Assurance and Cyber Security Directorate**
Location:	Wellington
Salary range:	G $68,316 - $102,474, H $77,711 - $116,567, I $90,366 - $135,548

Purpose of position:
The Cyber Incident Responder provides technical analysis during forensic investigations, as well as mitigation advice to victims of cyber intrusions

---

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 • Maintain an understanding of threat actor tactics, techniques and procedures (TTPs) • Maintain an understanding of attack tool capabilities and infrastructure • Conduct technology-based research projects, incorporating classified and open source material to ensure individual knowledge is class leading	• GCSB remains aware of cyber threat actors' intentions and capabilities • NCSC (National Cyber Security Centre) is recognised as the foremost expert on Cyber security within New Zealand Government • Tools and Signatures used in incident response activities are up to date against cyber threats
Providing Incident Response Services • Contribute to (and in some cases leading) the detection, analysis and understanding of sophisticated cyber-attacks on victim networks • Assist with the triaging of cyber incidents, with other members of the NCSC as appropriate • Collect, handle, and document forensic evidence, in accordance with forensic principles • Contribute to (and in some cases leading) the analysis of forensic evidence to meet investigation goals • Develop, maintain, and improve technical understanding and analytic techniques. Provide briefings and accounts of these analytic techniques to NCSC colleagues, as appropriate	• Cyber incidents are appropriately understood and evaluated • Appropriate and sufficient evidence is collected, and exhibits are correctly handled and inventoried with full audit capabilities • Forensic analysis is conducted in support of investigative goals • Technical capability and information can be operated or deployed with confidence by GCSB and the victim • NCSC remains a leader in the area of Cyber expertise and knowledge within New Zealand
Delivery of Output • Contribute to the provision of technical answers to questions regarding the compromise of New Zealand victim networks • Develop and understand mitigation design, and advice • Enhance NCSC's relationship and reputation with customers and partners through professional representation and engagement • Communicate effectively with external customer and partner agencies	• NCSC provides timely and accurate technical advice and expertise • The content of NCSC's technical reporting and advice is unambiguous, and the implications of why it has been provided are clear • The result of technical analysis is documented • Customers (victims) are positively engaged in the investigative process, and are kept appropriately informed of investigative outcomes. Customer concerns and expectations are appropriately managed • Productive and enduring relationships are formed with domestic and international partners

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:	• Other NCSC and GCSB team members
External:	• NCSC Customers • IT service providers • Victim organisations • Domestic and International Partners

Person Specification	
Experience:	• Experience in IT security, computer forensics, penetration testing or network defence • Knowledge of corporate network architectures • Experience with forensic tools, processes and artefacts • Experience with network defence and networking tools • Knowledge of Windows and Linux operating systems • Experience with programming / scripting
Knowledge and Skills:	• Interest in, and enthusiasm for, computer security • Strong interpersonal and communications skills with the ability to relate effectively to

	both technical and non-technical people • Demonstrate sound judgement, tact and integrity in dealing with sensitive issues • A desire to work in a highly collaborative team environment • Excellent knowledge of network protocols or host internals • Software engineering and programming • Demonstrates a practical and robust troubleshooting philosophy • A commitment to the documentation of process and actions • Results orientated with a demonstrable commitment to perform • Thinks critically and logically • The ability to be self-motivated, flexible and a team player • An ability and desire to learn new and sometimes complex skills • Excellent organisational skills and the ability to prioritise and work to deadlines • Displays initiative and self-confidence • 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 • Professional computing/networking qualification, e.g. in computer networking, or systems administration • Professional Information Security certifications
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.

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: 1/02/2019

Signatures		
Manager's Name		
Signature		Date:

Employee's Name		
Signature		Date:

GOVERNMENT COMMUNICATIONS SECURITY BUREAU

BEYOND ORDINARY
We are. Are you?