GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

POSITION DESCRIPTION

Technical Lead – Incident Coordination & Response

Unit/Branch, Directorate: Cyber Threat Response (CTR)
Information Assurance and Cyber Security Directorate

Location: Wellington

Salary range: I $90,366 - $135,548

Purpose of position: The Technical Lead for Incident Coordination and Response is responsible for the supervision and leadership of the NCSC's Incident Coordination and Response Team (ICR), as well as assisting the Unit Manager in determining and achieving the strategic goals of the unit. The Technical Lead provides senior oversight of the triaging and response to cyber security incidents, the technical analysis conducted during forensic investigations, and the mitigation advice provided to victims of cyber incidents.

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.

BEYOND ORDINARY
We are. Are you?

New Zealand Intelligence Community
Te Rōpū Pārongo Tārehu o Aotearoa
nzic.govt.nz

Key accountabilities	Deliverables/Outcomes
Team Leadership • Effectively lead the Incident Response and Coordination Team, to enable successful results from the team. Promote a positive, cohesive team environment where individuals demonstrate the core values of the GCSB. Ensure any impediments are identified and rectified. • Enable individuals to complete their tasks through analytic, technical and personal development and training. • Ensure a technical training curriculum is designed and implemented for all team staff. • Effectively manage workloads to ensure they are appropriate to meet Unit objectives and staff abilities. • Ensure performance objectives, reviews and discussions are completed in line with GCSB policies and procedures for all direct reports. • In conjunction with CTR Unit Manager and ICSS address poor performance of employees and ensure that good conduct and discipline is maintained at all times and any issues are dealt with promptly. • Demonstrate the stated values of the organisation in all aspects of their representation of the team/GCSB.	• Staff are motivated and engaged with a clear understanding of the technical requirements that meet unit and organisational objectives. • Staff are appropriately trained to meet Unit objectives. • Team and staff performance is continuously monitored. Unit is performing to its expected potential and organisational values are represented appropriately and respectfully. Any variance is addressed fairly and within an appropriate timeframe.
Managing Section Output • Ensure that cyber security incidents are triaged and documented in a timely manner, and according to NCSC operational policy. • Manage and monitor the response to cyber security incidents, and assistance to potential victims, ensuring that the unit's evaluation and investigation services are conducted effectively and professionally. • Technical oversight of the detection and analysis of sophisticated cyber incidents on victim networks, as undertaken by Incident Responders. • Technical oversight of the collection, handling, and documentation of forensic principles. • Technical oversight of the analysis of	• CTR Unit provides timely and accurate technical advice and expertise. • The content of CTR Unit's technical reporting and advice is unambiguous, and the implications of why it has been provided are clear. • Accurate technical advice and expertise is provided as necessary. • Cyber incidents are appropriately understood and evaluated, and output is correctly prioritised to maximum customer and GCSB value. • Incidents are appropriately triaged to maximise NCSC value, resources and output. • Appropriate and sufficient evidence is collected, and exhibits are correctly

forensic evidence to meet investigation goals, and identifying and influencing prioritisation decisions within investigations and incident response. • Developing, maintaining, and improving technical understanding and analytic techniques. Provide briefings and accounts of these analytic techniques to NCSC colleagues, as appropriate. • Ensure that team output effectively meets customer requirements and expectations and is of the highest quality. • Manage and monitor the provision of technical answers to questions regarding the compromise of New Zealand victim's networks. • Manage and monitor the development and understanding of mitigation design, advice and consequences.	handled and inventoried with full audit capabilities. • Forensic analysis is conducted in support of investigative goals. • CTR technical capability and information can be operated or deployed with confidence by GCSB and the victim. • CTR remains a leader in the area of Cyber expertise and knowledge within New Zealand.
Customer & Partner Liaison • Enhance GCSB's relationships and reputation with customers and partners through professionalism, representation and engagement. • Develop and manage a range of relationships, at both a domestic and international level. Seek out and develop new customer and operational relationships, to further enhance CTR's capabilities and reputation. • Provide technical leadership and advice to customer, partner, and other entities. • Ensure that output capabilities and priorities are known to customers where appropriate. Assist customers in understanding the correct mechanisms for tasking the section, and ensure that outputs are tailored to meet customer needs.	• Productive and enduring relationships are formed with domestic and international partners. GCSB is noted as a valued partner within the 5-Eyes Cyber community, and the technical capability of CTR Unit is valued at the national and community level. • Customers (victims) are positively engaged in the investigative process, and are kept appropriately informed of investigative findings. Customer concerns and expectations are appropriately managed.
Maintaining Training and Technical Expertise • Maintain a comprehensive understanding of attack tool capabilities and infrastructure, as well as the cyber threat to New Zealand, in order effectively mentor Incident Responders, Forensic Investigators and Incident Coordinators. • Maintain and improve technical understanding and expertise through	• GCSB remains aware of Cyber threat actors' intentions and capabilities. • Personal technical competency is retained. • NCSC technical capability and information can be operated or deployed with confidence by GCSB and the victim. CTR continues to improve and lead forensic analysis techniques.

continuing education. • Maintain a personal technical research and development portfolio, and also monitor and support research and development projects assigned to Incident Responders. • Monitor external drivers, and technology trends that are likely to impact CTR Unit business and stakeholders. • Develop and articulate technical strategic direction for the Unit. Identify and influence growth and business opportunities.	• NCSC remains a leader in the area of Cyber expertise and knowledge within New Zealand. • Research is relevant, and aligned to Unit objectives. • The Unit continues to improve and refine its operations. The Unit continues to develop new business areas. • Unit procedures are regularly reviewed and kept current to reflect contemporary practices.
Contribute to the execution of the IACD Operational Plan • Seek out the expertise of other colleagues and units to support your work, and offer your support to enhance theirs. • Create opportunities to involve customers in the design, delivery and evaluation of our services and work programmes; and/or support and participate in those opportunities as they arise.	• Engages across NZIC to create early collaboration as a means of setting the scene for later success. • Remains involved in customer engagements even when not in a position to drive them (e.g. participates in customer workshops; seeks feedback when providing services; identifies constructive response to negative customer feedback; identifies gaps in our knowledge about what customers require.
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. **Health and safety (for team):** • Inform, train and equip staff to carry out their work safely. • Ensure prompt and accurate reporting and investigation of all workplace incidents and injuries. • Assess all hazards promptly and ensure they are managed.	• 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 • Other GCSB staff as required
External:	• NZ Government Agencies • Organisations of national significance • International Intelligence and Law Enforcement partners • Other national or international forensic investigators and incident responders • IT service providers • Victim organisations

Person Specification	
Experience:	• At least 10 years' experience in IT field, with 5 years' experience in IT security, forensics or network defence • In-depth experience with forensic tools, processes and artefacts • Experience with both UNIX / Linux and Windows operating systems • Experience with network defence and attack tools • Experience in mentoring and leading staff
Knowledge and Skills:	• Knowledge of the cyber threat environment • Software engineering and programming • Vulnerability assessment tools and techniques • Knowledge of NZIC goals, processes and systems • Excellent communication and interpersonal skills • Demonstrate sound judgement, tact and integrity in dealing with sensitive issues • Excellent organisation skills and the ability to prioritise and work to deadlines
Qualifications and Courses:	• Tertiary degree, or equivalent experience, in Computer Science, Computer Forensics,

	Computer Security or similar field • Professional certifications relating to Computer Forensic Analysis, Cyber Security, Information Security or similar 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 Frontline Leader 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: 13/05/2019

Signatures		
Manager's Name		
Signature		Date:

Employee's Name		
Signature		Date:

GOVERNMENT COMMUNICATIONS SECURITY BUREAU

BEYOND ORDINARY
We are. Are you?