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

Position Description

Cyber Threat Analyst

Business unit:	Cyber Threat Response (CTR) Information Assurance and Cyber Security Directorate
Position purpose:	The Cyber Threat Analyst is responsible for the research and analysis of cyber-related threats and events, and the subsequent reporting to domestic and international customers.
Direct reports:	Nil
Financial delegation:	Nil
Directorate overview:	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 high assurance services; information assurance policy and advice; and high-end cyber security services to detect and respond to such threats.

GCSB mission and values

Our mission

Protecting and Enhancing New Zealand's Security and Wellbeing.

Our values

Respect, Commitment, Integrity, Courage.

Information Assurance & Cyber Security Directorate vision and mission

Our vision

"*Protect New Zealand's vital information infrastructures"*

Our mission

- To be a team of confident professionals, admired for our innovation and regarded both domestically and internationally as leaders in the Information Assurance and Cyber Security sectors.
- To have a comprehensive understanding of the advanced, technology-borne attempts to target our vital information infrastructures and steal our secrets and intellectual property.
- To be confident about our ability to monitor these threats and either reduce harm directly through timely provision of assurance and technical services or help others to mitigate risks through authoritative policy and expert advice built on our unique capabilities.

Role specification

Key result areas

The position of Cyber Threat Analyst encompasses the following major functions or Key Result Areas:

- Understand the cyber threat environment
- Cyber Threat Analysis
- Delivery of Output
- Contribute to the execution of the IACD Strategic Plan

The requirements in the above Key Result Areas are broadly identified below:

Jobholder is accountable for:	Jobholder is successful when:
Understanding the cyber threat environment ■ Maintaining an understanding of the cyber threat to New Zealand. ■ Maintaining an understanding of attack tool capabilities and infrastructure. ■ Maintaining and improving technical awareness and literacy regarding cyber threats and forensic analysis.	■ GCSB remains aware of cyber threat actors' intentions and capabilities, and the CTR Unit remains aware of current computer network defence (CND) trends and how these might impact New Zealand. ■ NCSC remains the point of contact as the area of cyber security expertise and knowledge within New Zealand. ■ The CTR Unit retains a high standard of research and analysis of cyber threats.

Cyber threat analysis

- Lead the analysis of multi-source evidence to maintain awareness of cyber events and electronic attacks.
- Collect, collate and analyse cyber security events, incidents and investigative leads.
- Prepare, document, and maintain event reports, requests to/from customers, and contribute to the development of policy statements as required.
- Manage personal operational tasking, and remain aware of Unit-wide operational developments, to ensure timeliness and deliverables.
- Develop, maintain, and improve technical understanding and analytic techniques. Provide briefings and accounts of these analytic techniques to colleagues, as appropriate.

- The capabilities and intentions of adversaries are clearly understood.
- Analytic observations or answers enable GCSB to provide an enhanced CND service.
- The risk to New Zealand infrastructure is understood.
- Cyber security events are recorded, evaluated and responded to in a timely and efficient manner.
- The escalation of an incident, and initiation of an investigative response, is based on well documented decision making and event reporting.
- Briefings and reports are appropriately constructed and delivered to ensure a consistent and accurate message is delivered to all stakeholders.

Delivery of output

- Produce timely and relevant cyber security related reporting for customers, based on material obtained from CND systems, intelligence partners, and unclassified sources.
- Enhance GCSB's relationships and reputation with customers and partners through professional representation and engagement. Ensure output capabilities and limitations are known to customers where appropriate. Understand customer requirements and tailor outputs where appropriate.
- Communicate effectively with technical, legal, executive and leadership teams within GCSB, and within external customer and partner agencies.

- 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.
- Team product meets all required quality standards, as specified in relevant policy documentation.
- Team product does not violate compliance rules, and any inadvertent breaches are notified to Compliance and dealt with appropriately.
- Productive and enduring relationships are formed with domestic and international partners.
- CTR Unit has a detailed awareness of customers' needs and expectations.
- Customer and partner enquiries are attended to in a timely manner.

- **Contribute to the execution of the IACD Strategic Plan**

- Team silos are visibly reduced and the focus of staff shifts from their own Unit

- 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 Team 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 IACD Strategic Plan.

Plans to delivering Directorate-wide objectives.

- Customer feedback suggests the Strategic 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.

Note:

The above performance standards are provided as a guide only. The precise performance measures for this position will need further discussion between the jobholder and manager as part of the performance development process.

Person specification

Qualifications

Essential:

- A tertiary qualification incorporating Computer Security study and/or equivalent experience; OR
- A tertiary qualification or equivalent experience incorporating technical analysis, problem solving, and report writing.

Knowledge/experience

Essential:	Desirable:
■ A background in intelligence analysis, cyber security or information assurance. ■ Excellent written communication skills and an ability to analyse and summarise data. ■ Presentation, public speaking or training skills and experience.	■ A good understanding of intelligence production and delivery mechanisms especially with regard to CND product.

Core competencies

All employees are measured against the following core competencies as part of performance development.

- Security
- Teamwork and Leadership
- Results Focus
- Communication and Knowledge Sharing
- Professionalism
- Innovation
- Customer Focus

Personal attributes

- 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.
- Demonstrate sound judgment, tact and integrity in dealing with sensitive issues.
- Excellent organisational skills and the ability to prioritise and work to deadlines.

- Displays initiative and self-confidence.
- The resilience to operate under pressure and correctly identify and asses risk, and make justifiable operational decisions.

Change to position description

Positions in GCSB may change over time as the organisation develops. Therefore, we are committed to maintaining a flexible organisation structure, which best enables us to meet changing market and customer needs. Responsibilities for this position may change over time as the job evolves.

Such change may be initiated as necessary by the manager of this position. This Position Description may be reviewed as part of the preparation for performance planning for the annual performance cycle.

Health & Safety

GCSB is committed to providing a healthy and safe work environment and safe management practices for all employees. Employees are expected to share this commitment as outlined in current Health and Safety legislation by taking all practicable steps to ensure:-

a. The employee's safety while at work, and

b. That no action or inaction of the employee while at work causes harm to any other person.

Knowledge Management

Employees are responsible for ensuring that all business records created are accessible and stored in the correct manner according to GCSB record keeping policy, standards and procedures.

Employee: _____ Date: _____

Manager: _____ Date: _____