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

Position Description

Cyber Incident Responder

Business unit:	Cyber Threat Response (CTR) Information Assurance and Cyber Security Directorate
Position purpose:	The cyber incident responder provides technical analysis during forensic investigations, as well as mitigation advice to victims of cyber intrusions.
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, mission and goal

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 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.

Functional relationships

External contacts:	Internal contacts:
▪ NZ Government agencies ▪ Organisations of national significance ▪ 2nd Party cryptologic agencies ▪ 2nd Party forensic groups ▪ Other national or international forensic investigators and incident responders ▪ IT service providers ▪ Victim organisations	▪ IACD staff ▪ GCSB IT security staff ▪ GCSB Intelligence staff ▪ NZSIS Investigations staff and State Intelligence Analysts ▪ Other GCSB/NZSIS staff as necessary

Objectives

The position of Cyber Incident Responder encompasses the following major functions or objectives:

- Understand the cyber threat environment
- Provide forensic services
- Delivery of Output
- Contribute to organisational processes and the execution of the IACD Operational Plan

The requirements in the above objectives are broadly identified below:

Jobholder is accountable for:	Jobholder is successful when:
Understanding the cyber threat environment ■ Maintaining a comprehensive understanding of networking tool capabilities and infrastructure in order to be an effective Incident Responder; ■ Conducting technology-based research projects, incorporating classified and open source material to ensure individual knowledge is class leading; ■ Maintaining a comprehensive understanding of the cyber threat to New Zealand.	■ GCSB remains aware of cyber threat actors' intentions and capabilities; ■ NCSC remains the point of contact as the area of Cyber expertise and knowledge within New Zealand; ■ Tools and Signatures used in forensic investigations are up to date against cyber threats.
Providing forensic services ■ Contributing to (and in some cases leading) the detection, analysis and understanding of sophisticated cyber-attacks on victim networks; ■ Assisting with the triaging of cyber incidents, with other members of the NCSC as appropriate; ■ Responsible for the collection, handling, and documentation of forensic evidence, in accordance with forensic principles; ■ Contributing to (and in some cases leading) the analysis of forensic evidence to meet investigation goals; ■ Developing, maintaining, and improving technical understanding and analytic techniques. Provide briefings and accounts of these analytic techniques to NCSC colleagues, as appropriate.	■ Cyber events 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 relationships and reputation with customers and partners through professional representation and engagement.	■ Provides timely and accurate technical advice and expertise; ■ The content of technical reporting and advice is unambiguous, and the implications of why it has been provided are clear; ■ The result of technical analysis is documented according to GCSB knowledge management procedures; ■ Customers (victims) are positively engaged in the investigative process, and are kept appropriately informed of

■ Communicate effectively with external customer and partner agencies.	investigative findings. Customer concerns and expectations are appropriately managed; ■ Productive and enduring relationships are formed with domestic and international partners.
<u>Contribute to the execution of the IACD Operational Plan</u> ■ Promoting cross-team collaboration through the execution of the IACD Operational 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 Operational 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.

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:	Desirable
■ Tertiary degree, or equivalent experience, in Computer Science, Computer Forensics, Software Engineering, or Computer Security	■ Qualifications in Incident Response or Malware Analysis ■ Successful completion of any available internal training on Forensic Analysis

Knowledge/experience

Essential:	Desirable:
■ Experience in IT security, computer forensics, or network defence. ■ Experience with operating systems, both UNIX / Linux and Windows. ■ Experience with forensic tools, processes and artefacts.	■ Experience with network defence and networking tools. ■ Software engineering and programming. ■ Vulnerability assessment tools and techniques.

Specialist competencies

The following would typically be expected for the 100% fully effective level:

- Network Intrusion Detection, Methods and Signature Development
- Host Forensics
- Malware Analysis
- Adversary Intentions and Methodology
- Penetration Testing
- System Administration
- Reverse Engineering
- Programming
- Networking

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

- Strong interpersonal and communications skills with the ability to relate effectively to both technical and non-technical people
- The ability to authoritatively and tactfully represent the GCSB when engaging with customers
- The ability to be self-motivated, flexible and a team player.
- Demonstrates a practical and robust troubleshooting philosophy.
- Thinks critically and logically.
- An ability and desire to learn new and sometimes complex skills.
- Demonstrate sound judgment, tact and integrity in dealing with sensitive issues.

- The resilience to operate under pressure and correctly identify and asses risk, and make justifiable operational decisions
- A commitment to the documentation of process and actions.
- Results oriented with a demonstrable commitment to perform.
- Excellent organisational skills and the ability to prioritise and work to deadlines.
- Highly effective planning and organisational skills.
- The ability to participate in management fora as an effective member of the team, and contribute to the development of a high performance organisation.
- The ability to represent the GCSB/NCSC with credit within national and international communities.

Change to position description

Positions in GCSB may change over time as the organization develops. Therefore, we are committed to maintaining a flexible organization 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 in Employment 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: _____