MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

POSITION DESCRIPTION

Position details	
Position Title	Senior Incident Manager/Analyst
Team/Branch/Group	CERT NZ/Service Support & Design/Market Services
Location	Wellington
Date	October 2016

Our purpose

Our purpose is to grow the New Zealand economy to provide a better standard of living for all New Zealanders. To achieve this, we need a strong, high performing economy, where for example, people (workers, consumers and investors) are protected and aware of their rights and obligations; and the integrity of the environment is maintained.

As one of New Zealand's largest government agencies, the work we do impacts the lives of all New Zealanders. We work to increase household incomes by helping businesses to be more productive and internationally competitive, increasing opportunities for all New Zealanders to participate in the economy through improved job opportunities, and by ensuring quality housing is more affordable.

This is all echoed in our Māori identity – Hikina Whakatutuki – which broadly means "lifting to make successful".

How we work

Our aspiration is that MBIE is a great place to work where great work gets done.

We believe in harnessing the potential of our people and the diverse skills and life experiences they bring to MBIE.

Our targets are challenging and require us to work with others, and across the Ministry (making the most of our size and scope).

Our people will need to adopt a generous disposition and actively seek out opportunities to be purposely collaborative across MBIE. This means asking 'why not?' instead of 'why?', and leveraging off the collective that is MBIE in the pursuit of goals that stretch right across teams, branches and groups.

We work across government, and New Zealand, in a way that enables us to expand and deepen our understanding of businesses and markets. We use our extensive presence across New Zealand and around the world to make and leverage domestic and global connections.

With our Crown entity partners we work collaboratively with other government agencies; local government; businesses; industry, sector, union and employer groups; consumer groups; Māori leaders; and scientists to develop and deliver fit-for-purpose policy, services, advice and regulation that support people, businesses, communities and regions to be successful.

As the lead agency for providing government services for business, we are focussed on making it easier for business to interact with government.

Our character

Shape We shape the agenda by challenging the status quo, and by generating and adopting new ideas, to bring those ideas to life.

Collaborate	We support each other, engage early and proactively partner in pursuit of shared goals.
Deliver	We have a can do attitude, take ownership, act with purpose, urgency and discipline, take calculated risks, celebrate success and learn as we go.

Our structure

The Ministry comprises around 3,200 staff operating in New Zealand with a further 400 staff in overseas locations.

The Ministry has seven business groups: Building, Resources and Markets; Corporate, Governance and Information; Finance and Performance; Immigration New Zealand; Labour, Science and Enterprise; Market Services; and the Office of the Chief Executive.

The Senior Incident Manager position reports into the Operations Manager within CERT NZ which is part of the Market Services business group.

The functions in the Market Services group are:

- CERT NZ
- Resolution Services
- Service, Support & Design
- Consumer Protection & Standards
- Business Integrity Services
- Better for Business (R9)
- NZ Government Procurement & Property
- Integrated Regulatory Enforcement (IREB)
- Labour Inspectorate
- Business Management

Service Support and Design Branch

The branch is critical to ensuring the Group delivers efficient, effective and value-added services to consumers and business. It is responsible for leading or supporting the delivery of transformative cross-MBIE and cross-Government programmes, creating a critical mass of capability to underpin fact-based systemic thinking, innovation and smarter service delivery across the group. It is responsible for leading the cross-Group business analysis and leading performance management, systems improvements, and championing service transformation programmes.

CERT NZ

The establishment of a national CERT is a key element of New Zealand's Cyber Security Strategy 2015 and will contribute to the delivery of the Strategy's vision of 'A secure resilient and prosperous online New Zealand'.

A CERT is an organisation that receives cyber incident reports, tracks cyber security incidents or attacks, and provides advice and alerts to its customers on how to respond and prevent further attacks. CERTs also work closely with their international counterparts to prevent and respond to cybersecurity incidents, and address cybercrime.

The CERT is staffed with passionate Cyber Security Experts and experienced Communications and Engagement staff, providing services from 7am to 7pm Monday to Friday and a 24/7 response to serious cyber incidents which means at times being called upon out of hours in an emergency.

Establishing a national CERT means New Zealand joins an international network of CERTs, improving our access to information on potential or real-time cyber-attacks. It will help New Zealand play our part in a global effort to improve internet security. Ultimately, New Zealand will become a more trusted business and security partner.

Position purpose

The Senior Incident Manager is responsible for taking the lead on triaging, managing and investigating cyber incidents which will include ensuring that appropriate advice is sent out to affected parties, to warn them and

inform them on how to mitigate the threat. The Senior Incident Manager will also, from time to time, be expected to represent New Zealand at international cyber security conferences as an expert on incident management.

Key relationships

- CERT NZ Operations Manager
- CERT NZ Management Team
- Staff within CERT NZ
- Government agencies, including the National Cyber Security Centre, NZ Police, and the Department of Internal Affairs
- Tier 2 & 3 managers across the public and private sectors
- International CERTs
- Service providers

Key accountabilities and deliverables

Responsibilities of this position are expected to change over time as the Ministry responds to changing needs. The incumbent will need the flexibility to adapt and develop as the environment evolves.

Key accountability or deliverable	**Indicators of success**
Critical areas of success *Delivers quality results which contribute to the Ministry's outcomes*	The Senior Incident Responder will be required to deliver results in the following areas: • Directing the development and maintenance of the incident management systems • Responsible for planning and coordinating all the activities required to manage and analyse incidents, including serious national Incidents, including: o Triage and response to incidents o Interpreting threat intelligence o Incident referral (Domestic & International) o Prepare, document and maintain incident reports and investigative plans • Serious cyber incident response and coordination, including: o Leading the unit's response, and thereby being instrumental in the coordination of New Zealand's overall response to serious cyber incidents o Conducting and Supporting briefings to senior executives o Communicating with technical and non-technical audiences o Holding the lead coordination role for New Zealand's response for shift-based periods. • Identifying opportunities for continuous improvement, and establishing processes to review and enhance services and activities • Represent New Zealand as the expert on incident management at international cyber security conferences • Inform responses to inquiries from the media on cyber security events/issues • Engage and develop direct collegial relationships with other international CERTs staff to ensure the exchange of information

Key accountability or deliverable	Indicators of success
	• Developing and maintaining the serious cyber incident response process and associated procedures • Managing the interface between classified and unclassified environments • Providing advisories on threats and vulnerabilities the public and other stakeholders on threats
Stakeholder Management *Manage constructive working relationships with internal and external stakeholders to enhance understanding and co-operation needed to achieve desired results.*	• Relationships are established, maintained and enhanced with relevant clients and stakeholders. • Transfers knowledge and learning to the team and wider organisation. • Timeliness of delivery is effectively managed to meet business and stakeholder needs. • Issues and risks are identified and managed. • Represents whole-of-Ministry views and protects its reputation in any external interactions.
Safety and wellbeing *Manages own personal health and safety, and takes appropriate action to deal with workplace hazards, accidents and incidents.*	• Displays commitment through actively supporting all safety and wellbeing initiatives. • Ensures own and others safety at all times. • Complies with relevant safety and wellbeing policies, procedures, safe systems of work and event reporting. • Reports all incidents/accidents, including near misses in a timely fashion. • Is involved in health and safety through participation and consultation.
Competencies	
Cultivates Innovation	**Shape the agenda**, creating new and better ways for the organisation to be successful, by • Coming up with useful ideas that are new, better or unique • **Challenging the status quo** • Introducing new ways of looking at problems • **Generating and adopting new and creative ideas**, and putting them into practice • Encouraging diverse thinking to promote and nurture innovation
Nimble Learning	Actively learn through experimentation when tackling new problems, using both successes and failures as learning fodder, by • **Learning as we go,** when facing new situations • Experimenting to find new solutions • Taking on the challenge of unfamiliar tasks • Extracting lessons learned from failures and mistakes • Being flexible and responsive to changes in requirements • Identifying personal learning opportunities • Finding own solutions where possible
Collaborates	**Support others,** building partnerships and working collaboratively with others to meet shared objectives, by • Working co-operatively with others across MBIE, the public sector and external stakeholder groups to achieve shared objectives • Balancing competing interests and priorities appropriately and in line with MBIE's priorities • Identifying, **engaging early** and partnering with relevant stakeholders to get work done • Crediting others for their contributions and accomplishments • Gaining trust and support of others.

	• Addressing behaviours that do not align with our culture • Seeking and respecting the views and opinions of others • Providing timely and helpful information to others across the organisation
Customer Focus	Build strong customer relationships and delivering customer-centric solutions, by • Gaining insights into customer needs • Delivering quality, accurate, timely service and customer focussed solutions • Identifying opportunities that benefit the customer and will improve service delivery • Building and delivering solutions that meet customer expectations • Establishing and maintaining effective customer relationships • **Pro-actively partnering in pursuit of shared goals.** • Actively seeking and responding to customer feedback
Action Oriented	Take on new opportunities and tough challenges with **purpose, urgency and discipline,** by • Readily **taking ownership** and action on challenges, without unnecessary planning, and being accountable for the results • Identifying and seizing new opportunities • Displaying a **can-do attitude** in good and bad times, and **celebrating success** • Stepping up to manage tough situations and encouraging my colleagues to do the same
Decision Quality	Make good and timely decisions that keep the organisation moving forward, by • Making sound decisions, even in the absence of complete information • Relying on an appropriate mix of analysis, wisdom, experience and judgement to make valid and reliable decisions • Considering all relevant factors and using appropriate decision-making criteria and principles, **taking calculated risks** where required • Recognising when a quick 80% solution will suffice, and when it will not • Analysing information to make effective decisions in order to improve performance
Organisational commitment and public service	Role models the standards of Integrity and Conduct for the State Services Contributes to the development of, and helps promote and builds commitment to MBIE's vision, mission, values and services, by • Willingly undertaking any duty required within the context of the position • Managing own personal health and safety, and takes appropriate action to deal with workplace hazards, accidents and incidents • Understanding Equal Employment Opportunities (EEO) principles and the application of these to MBIE • Complying with all legislative requirements and good employer obligations

Personal specifications

- Strong experience in incident response
- Experience with network and system security analysis
- Experience in computer network defence and operating in a hostile environment
- Comprehensive understanding of cyber threats and the threat landscape
- Experience with the interpretation and application of threat intelligence
- A solid understanding of security controls and how to mitigate threats
- Sound knowledge of STIX and TAXII standards
- Experience in penetration testing
- An understanding of digital forensics
- Must have the legal right to live and work in New Zealand
- Must hold an existing government security clearance or be able to obtain and maintain a security clearance