JOB DESCRIPTION

Specialist Digital Threat Assessment

ROLE TITLE	Specialist Digital Threat Assessment
SECTION/DIVISION:	IT Assurance and Cyber Security, Digital Division
REPORTS TO:	Senior Manager Security Operations
DIRECT REPORTS (FTE):	Nil
INDIRECT REPORTS (FTE):	Nil
PRIMARY PURPOSE OF THE ROLE:	The Digital Threat Specialist monitors and responds to online threats targeting the University's brand, staff, and information assets across platforms including social media, forums, and the dark web. Using intelligence tools and investigative techniques, the role identifies and addresses risks such as impersonation, misinformation, and staff abuse. Working closely with security, legal, communications, and affected individuals, the specialist ensures early threat detection, effective incident response, and promotes online safety through education and collaboration.
ACCOUNTABILITIES:	**Threat intelligence, THIN: Level 4** Collates and analyses information for threat intelligence requirements from a variety of sources. Contributes to reviewing, ranking and categorising qualitative threat intelligence information. Creates threat intelligence reports. Evaluates the value, usefulness and impact of sources of threat intelligence sources. **Specialist advice, TECH: Level 4** Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations. Actively maintains knowledge in one or more identifiable specialisms. Recognises and identifies the boundaries of their own specialist knowledge. Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs. **Security operations, SCAD: Level 2** Receives and responds to routine requests for security support. Maintains records and advises relevant persons of actions taken. Assists in the investigation and resolution of issues relating to access controls and security systems. Documents incident and event information and produces incident, exception, and management reports. **Information security, SCTY: Level 3** Applies and maintains specific security controls as required by organisational policy and local risk assessments.

Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems.

Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures.

Supports investigation of suspected attacks and security breaches.

Learning delivery, ETDL: Level 3
Delivers learning activities to a variety of audiences using prepared materials to meet established learning objectives.

Uses established guidelines for the preparation of the environment. Assists with the development and maintenance of examples and case study materials.

Appropriately uses a range of learning delivery techniques to enable learners to develop skills, capability, techniques and required knowledge.

Observes learners performing practical activities and work. Advises and assists where necessary. Provides detailed instruction where necessary and responds to questions, seeking advice in exceptional conditions beyond own experience.

Vulnerability assessment, VUAS: Level 3
Follows standard approaches to performs basic vulnerability assessments for small information systems.

Supports creation of catalogues of information and technology assets for vulnerability assessment.

KEY RELATIONSHIPS:

Internal
IT Services Division staff
Comms Team
Staff
Students

External
Industry and tertiary sector peers
Government agencies such as NZ Police, Department of Internal Affairs
Internet Service Providers
Vendors, service providers, contractors, consultants

QUALIFICATIONS AND EXPERIENCE:

Essential
Tertiary level Computer Science qualification or equivalent discipline
Considerable experience in threat intelligence or digital risk monitoring, with a background in security operations or incident response, as well as conducting investigations into impersonation, misinformation, or digital abuse.
Practical knowledge of information security controls, incident logging, and basic risk assessments.
Demonstrated experience engaging respectfully with stakeholders and working collaboratively across a range of disciplines.

Preferred
Experience in delivery of learning materials and support to community members.
Postgraduate qualifications or certifications in cyber security, quality assurance, compliance, or business continuity (e.g. Certified Internal Auditor (CIA), or Certified Information Systems Auditor (CISA), are highly valued.
Experience in leading and advocating the use of Te Reo, tikanga and mātauranga Māori in the workplace.
Experience in higher education, government, or other public-sector environments.

TECHNICAL SKILLS AND KNOWLEDGE:	Proficient in OSINT tools and threat intelligence analysis to identify and assess digital threats across social media, forums, and dark web sources. Experience with incident detection and response, including SOC operations and security event monitoring. Strong understanding of information security fundamentals, vulnerability assessments, and cyber hygiene best practices. Knowledge of New Zealand regulatory requirements relevant to the education sector, public sector governance, privacy, and health and safety. Experience delivering digital threat awareness and training to diverse audiences.
SPECIAL REQUIREMENTS:	Some travel may be required to attend other sites. After hours or on - call work will be required on occasion. A police vetting check from a relevant agency satisfactory to the University will be a condition of employment. At the University, we are required to be compliant with the Public Records Act 2005 and Privacy Act 2020. Staff are expected to participate in available training to understand these requirements and effectively manage information accordingly.
DIRECT BUDGET ACCOUNTABILITY:	Nil
MĀORI STRATEGIC FRAMEWORK:	Act in a manner consistent with the principles and implications, as well as the University's commitment to the Treaty as articulated in the Māori Strategic Framework.
PACIFIC STRATEGIC FRAMEWORK:	Act in a manner consistent with the strategies and goals contained in the University's Pacific Strategic Framework, role-modelling and promoting Pacific values, equity and diversity principles and cultural safety practices.
HEALTH AND SAFETY:	Act and work in a manner compliant with current health and safety at work legislation and University procedures, frameworks and guidelines. Role model safe behaviour and practices, share the responsibility to prevent harm and contribute to a safe campus and work environment, including raising workplace health and safety concerns for self, students, visitors and other staff.
SUSTAINABILITY:	Act in a manner consistent with the University's sustainability commitments; role-modelling sustainable practices, with a particular emphasis on minimising the environmental impact of day-to-day activities.

SKILLS FRAMEWORK FOR THE INFORMATION AGE (SFIA)

Specialist Digital Threat Assessment

Role Type: Specialist

SFIA Levels of responsibility

Autonomy	3	Influence	4	Complexity	3	Business Skills	4	Knowledge	4

SFIA Skills Profile

Category	Subcategory	Skill	Code	L1	L2	L3	L4	L5	L6	L7
Strategy and architecture	Security and privacy	Threat intelligence	THIN				■			
Strategy and architecture	Advice and guidance	Specialist advice	TECH				■			
Delivery and operation	Security services	Security operations	SCAD		■					
Strategy and architecture	Security and privacy	Information security	SCTY			■				
People and skills	Skills management	Learning delivery	ETDL			■				
Delivery and operation	Security services	Vulnerability assessment	VUAS			■				

https://help.sfia.nz/hc/en-nz/sections/4407230514201-Levels-of-responsibility

https://sfia-online.org/en/sfia-8/sfia-views/full-framework-view?path=/glance