POSITION DESCRIPTION

Senior Cyber Threat Intelligence Analyst

POSITION DETAILS

Position Title	Senior Cyber Threat Intelligence Analyst
Classification	HEW 8
Position Number	7013275
School/Office	Digital Services / Security & Digital Operations
Division	Division of Operations

POSITION PURPOSE

The Senior Cyber Threat Intelligence Analyst role is responsible for delivering expert threat intelligence analysis and operational support to enhance the University's cyber defence capabilities. The position contributes to the development and integration of threat intelligence into security operations, enabling proactive identification and mitigation of emerging threats. Operating within a complex digital environment, the role supports strategic initiatives and ensures alignment with institutional risk posture and sector standards.

The role acts as a senior advisor on threat intelligence, providing situational awareness of adversary tactics, techniques, and procedures (TTPs). It ensures intelligence outputs inform decision-making across governance, risk, and compliance, and directly strengthen incident detection and response. The Senior Cyber Threat Intelligence Analyst position also plays a pivotal role in representing the University in national and sector intelligence forums, contributing to the uplift of collective cyber resilience.

KEY ACCOUNTABILITIES

- Conduct advanced threat intelligence analysis to identify emerging cyber risks and inform defensive strategies.
- Develop and maintain threat intelligence feeds and indicators of compromise (IOCs) relevant to the University's technology landscape.
- Integrate threat intelligence into security operations workflows, supporting proactive detection and response.
- Collaborate with internal stakeholders to ensure intelligence outputs align with operational needs and compliance requirements.
- Contribute to cyber incident investigations, providing contextual intelligence and adversary

profiling.
- Support the development of threat modelling frameworks, including MITRE ATT&CK and kill chain methodologies.
- Maintain relationships with external intelligence-sharing communities, including sector partners and government bodies.
- Prepare intelligence briefings and reports for technical and executive audiences.
- Ensure threat intelligence activities are embedded in University cyber risk management processes, providing inputs to governance, assurance, and compliance reporting.
- Champion the adoption of automation, AI-driven analytics, and advanced tooling to increase the effectiveness and timeliness of intelligence outputs.

QUALIFICATIONS, EXPERIENCE AND SKILLS

- Tertiary qualifications in Cyber Security, Information Technology, or a related discipline.
- Demonstrated experience in cyber threat intelligence, including analysis, reporting, and operational integration.
- Strong understanding of threat intelligence frameworks and adversary tactics.
- Experience with threat modelling tools and methodologies.
- Excellent analytical and communication skills, with the ability to translate complex intelligence into actionable insights.
- Proven ability to contribute to incident response with timely and context-rich threat intelligence.
- Experience in representing organisations in intelligence-sharing communities or government/sector forums.

Technical Proficiency

- Hands-on experience with cyber threat intelligence platforms (TIPs), SIEM/SOAR tools, and open-source intelligence (OSINT) frameworks.
- Proficiency in using and interpreting structured intelligence standards (e.g., STIX/TAXII).
- Familiarity with MITRE ATT&CK, Cyber Kill Chain, Diamond Model, or similar frameworks.
- Experience with automation/scripting for enrichment and correlation of threat data (e.g., Python, PowerShell).

Desirable

- Industry certifications (e.g. CTIA, GCTI, CISSP) are desirable.
- Experience in higher education, government, or critical infrastructure sectors.
- Knowledge of national cybersecurity frameworks and reporting requirements (e.g., ACSC Essential Eight, ISM).

KEY RELATIONSHIPS

This position reports to: Principal Cyber Threat Intelligence

This position supervises: None

Key internal relationships:

- Information Technology and Digital Services
- Cyber Security Assurance and Operations
- Office of General Counsel

- Audit and Risk

Key external relationships:

- Australian Cyber Security Centre
- Sector partners and peer institutions
- Relevant government and regulatory bodies

CHALLENGES

- Synthesising complex threat intelligence into actionable operational outputs.
- Maintaining situational awareness across diverse and evolving threat landscapes.
- Ensuring intelligence practices comply with regulatory and legislative frameworks.
- Supporting incident response with timely and relevant intelligence.

OCCUPATION SPECIFIC CAPABILITY SET

SFIA

Capability Name	Code	Level	Rationale
Threat intelligence	ININ	5	Conducts advanced threat intelligence analysis and integrates findings into security operations to proactively identify and mitigate risks.
Incident management	USUP	5	Provides contextual intelligence during incident investigations, enabling faster and more accurate response.
Information security	SCTY	5	Ensures threat intelligence practices align with institutional risk posture, governance, and compliance standards.
Research	RSCH	5	Supports development of threat modelling frameworks (e.g., MITRE ATT&CK, kill chain) and applies structured research methodologies.
Analytics	INAN	5	Synthesises complex threat data into actionable insights and produces intelligence briefings for diverse audiences.
Stakeholder management	RLMT	5	Collaborates with internal teams and maintains relationships with sector and government intelligence-sharing communities.
Emerging technology monitoring	EMRG	5	Evaluates and applies emerging tools, automation, and AI analytics to enhance intelligence capabilities.
Mentoring	MENT	4	Provides technical mentoring to junior analysts, supporting capability uplift and professional development.

UNIVERSITY EXPECTATIONS

The University expects that all employees are aware of, and comply with legislation and Western's policies and procedures relevant to the position, including but not limited to:

→ Code of Conduct
→ Work Health and Safety and Wellbeing Management System
→ Enterprise Agreement or Award
→ Anti-discrimination principles, Equal Employment Opportunity and staff and student equity.

Approved by:
Date: