POSITION DESCRIPTION

Murdoch University

Position	**Senior Cyber Operations Analyst**
Level / Classification	HEW0808
Reports to	Head of IT
Unit	Digital & Technology > IT Operations
Directorate	Chief Experience Office
Positions Supervised	Nil

Position Purpose

The Senior Cyber Operations Analyst provides technical leadership within the Cyber Operations team, with primary responsibility for the effective operation, administration, and continuous improvement of the University's cyber security technologies and controls. The role plays a key part in uplifting security capability and maturity by identifying gaps, driving remediation activities, and contributing to the design and implementation of new security technologies.

Working under the direction of the Cyber Operations Lead, the role leads and validates operational security activities including security monitoring, vulnerability management, threat detection and response, and information security investigations. This includes acting as a technical escalation point for complex incidents, providing expert guidance during high-risk security events, and coordinating investigation, containment, and remediation activities across the team.

The Senior Cyber Operations Analyst also acts as a technical authority for security tooling and detection capability, providing subject matter expertise on configuration, architecture, and detection logic. The role contributes to governance and assurance activities by ensuring security operations align with policy requirements, supporting audits, and providing evidence and technical input as required.

In addition, the role is responsible for uplifting team capability through mentoring, coaching, and knowledge transfer, as well as improving operational processes through the development and maintenance of runbooks, workflows, and reporting. The Senior Cyber Operations Analyst works closely with the Digital and Technology team and collaborates with

other University staff and students as required to strengthen the University's overall security posture.

About Murdoch University

Murdoch University is a young and dynamic university with a foundational commitment to the environment, social justice and inclusion, and making education accessible to more people. Founded as Western Australia's second university in 1974, today, Murdoch has more than 21,000 students and 1,700 staff across campuses in Perth, Singapore and Dubai. With more than 90,000 Alumni, Murdoch graduates can be found all over the world, making a positive difference.

Our Strategy – *Ngala Kwop Biddi. Building a brighter future, together* – guides the University's direction and reaffirms our shared purpose to change lives and society for the better through accessible education and research.

The Strategy is focused on three key themes:

- Sustainability: Be a leading university in education, teaching and translational research in sustainability.
- Equity, Diversity, and Inclusion: Build a welcoming, diverse and inclusive community.
- First Nations: Become the University of first choice for First Nations peoples.

Murdoch is also committed to building engagement with our local community, State, nation, and global society with a track-record in creating strong partnerships with business, government and industry.

About the Work Area

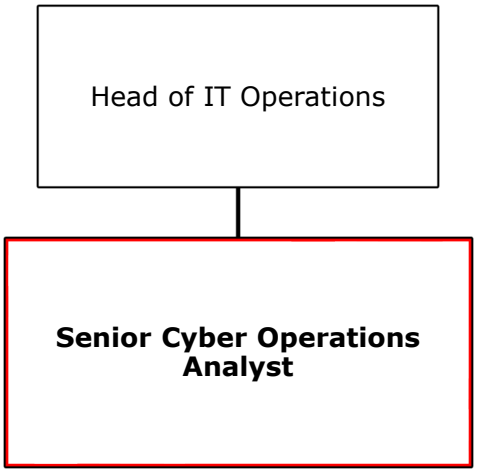
Digital & Technology are a critical partner in delivering innovative technology leadership and delivery excellence in advancing the University's strategic goals. Our teams provide key services across:

- Operations
- Planning and Governance
- Solutions Delivery

In support of our university strategy, *Ngala Kwop Biddi*, Digital and Technology seeks to drive the transformation of a truly innovative digital technology experience in creating a vibrant campus for business, industry, start-ups, health sectors, local and global investors, researchers, students, alumni and the broader community to come together to learn, innovate, and collaborate.

The Cyber Team is a critical component in protecting Murdoch University's digital assets.

Reporting Relationships



Key Responsibilities/Duties

1. Lead the maintenance and improvement of security technologies to identify and reduce information and computer security risk.
2. Review security posture and technology usage. Identifying and gaps and driving remediation priorities.
3. Direct, validate and correlate data collection for investigations and report security weaknesses to appropriate support teams.
4. Manage and monitor the efficacy of Indicators of Compromise in the security toolset.
5. Monitor for and respond to high-risk security threats, events and alerts. This include providing guidance in complex investigations and providing and escalation point for the team.
6. Responsible for the administration and management of security technologies including upgrades, patching, configurations, reporting, user and privilege management. This includes input into configuration design and architecture.
7. Provide detailed analysis reporting on security performance against established metrics and SLAs.
8. Providing advice on innovative security technologies by coordinating technical delivery, making configuration and detection decisions and acting as technical authority.
9. Lead the technical analysis, containment and remediation of security incidents. This includes coordinating team response and drive post incident lessons learned and improvements.
10. Provide capability uplift of team, runbooks, workflows and reports. This includes mentoring, coaching and knowledge transfer of technical skills to other Cyber team members.

11. Provide light governance alignment. This includes ensuring technology operations align to policy, providing support for audits and assurance activities, providing evidence and subject matter input.
12. All other duties as required.

Selection Criteria

Essential

1. A degree in Cyber Security or similar IT discipline with some relevant experience or an equivalent combination of relevant experience and/or education/training.
2. Experience in security technologies such as Endpoint Protection, SIEM, vulnerability management, firewalls and networking.
3. Knowledge of security incident response and problem-solving techniques including log analysis, forensic analysis and root cause analysis
4. Strong knowledge in Microsoft Defender Suite, with experience in Defender for Endpoint or similar applications.
5. Good experience in Microsoft Purview, scripting and KQL Coding or similar.
6. Strong analytical skills and ability to articulate findings and ideas to peer group.
7. Ability to build strong relationships and communicate effectively with stakeholders of all levels.
8. Excellent verbal and written skills.

Desirable

1. Experience in a similar position in a university or similar complex large organisation.
2. Industry certification in relevant field.
3. Relevant industry associations related to Cyber Security or IT Service Management.

Work Requirements

1. Australian permanent residency or possession of a valid visa with work entitlement in Australia.
2. The occupant of this position will be required to undertake a criminal record check in accordance with the University's Employee Background Checks Procedure.
3. Some after-hours work may be required.
4. Ability to work outside of normal office hours that may include occasional weekend work when required.

General Obligations

While at work, an employee must:

- take reasonable care for their own health and safety and ensure that their acts or omissions do not adversely affect the health and safety of other persons;
- report incidents, injuries and hazards;
- comply with any reasonable instruction that is given by Murdoch University; and
- comply with Murdoch University policies and procedures.

Guiding Principles and Values/Code of Ethics and Code of Conduct

Our Values

- Authenticity
- Integrity
- Respect
- Inclusivity
- Openness

Our Principles

- Act with justice, respect and responsible care.
- Be collegiate and respectful of other points of view.
- Protect academic freedom.
- Be agile, flexible and resilient.
- Make decisions at the most appropriate level.
- Be transparent in decision-making and with information.
- Adopt common approaches to common tasks.
- Be careful stewards of our resources.

All staff will comply with the University's Code of Ethics and Code of Conduct and demonstrate a commitment to its Equity, Diversity and Safety principles and the general capabilities of personal effectiveness, working collaboratively and demonstrating a focus on results.

All Staff complete a Development Review annually. A Commencing Development Review should be completed within 3 months of commencement.

We acknowledge that Murdoch University is situated on the lands of the Whadjuk and Binjareb Noongar people. We pay our respects to their enduring and dynamic culture and the leadership of Noongar elders past and present. The boodjar (country) on which Murdoch University is located has, for thousands of years, been a place of learning. We at Murdoch University are proud to continue this long tradition.