**POSITION DESCRIPTION**

|  |  |
| --- | --- |
| **Position Description Classification Approved** | **Date** |
| Human Resources Branch | 13/6/2024 |

|  |  |
| --- | --- |
| **POSITION DETAILS** |  |
| **Position Title:** | **Senior Cyber Security Analyst** |
| **Position Number:** | 00026404 |
| **Classification:** | HEO 8 |
| **Faculty/Division:** | Division of University Operations |
| **School/Branch:** | Information Technology and Digital Services (ITDS) |
| **Reports to (position title):** | Cyber Security Operations Lead |
| **Delegations:** | N/A |
| **Special Conditions:** | * Participate in the on-call roster as required. * Attend meetings and work outside of standard hours as required. * Primary place of employment is the North Terrace campus, but may be required to work at all University campuses and facilities (including hospitals) where University staff and students reside. * Reasonable workplace adjustments will be made for people with a disability. * Evidence of a satisfactory National Police Check/Certificate is required prior to making an appointment to this position. |
| **Significant Working Relationships:** | * IT Operations teams. * IT Strategy, Planning and Governance teams. * All University staff and students. * Legal & Risk. * Human Resources. * Internal & External Stakeholders. |

|  |
| --- |
| **POSITION SUMMARY** |
| The University of Adelaide is a large and successful university in Australia's Group of Eight research intensive universities, distinguished by its international reputation and commitment to innovation and excellence in research and teaching.  The Information Technology and Digital Services Branch is a part of the University’s Division of University Operations, which provides enabling services and resource capabilities to support the University’s teaching and research objectives and activities. ITDS provides services and support to the University of Adelaide community of over 25,000 students and 3500 staff members.  ITDS is responsible for the development and implementation of the strategy and framework to ensure that learning & teaching staff, students, and researchers at the University are aware of and get maximum benefit from digital technologies, infrastructure and learning & teaching and research tools and facilities available to the University.  Operating within the IT Architecture and Information Security Department the Information Security team provides a range of services including security governance, security awareness and training, security testing, incident detection and response, investigations, and digital identity and access management. The mission of the team is to (i) protect the security of teaching, learning, and research data across the University (ii) enable the University to innovate by managing risks and (iii) foster a security-aware culture, engender trust, and protect the established brand.  Receiving broad direction and working with a degree of autonomy, the Senior Cyber Security Analyst provides fundamental operational security support, including daily proactive monitoring and validation of alerts, responding to customer requests and reports, performing vulnerability scans, maintenance of the security toolset, performing/executing penetration testing, and responding to both potential and actual security incidents. The Senior Cyber Security Analyst plays a vital role in maintaining a sustainable security operations capability by assisting the development and training of junior security operations staff as well as communicating effectively with stakeholders inside and outside of the ITDS branch. |

|  |  |
| --- | --- |
| **KEY RESPONSIBILITIES** | |
| Security Operations | * Perform threat intelligence activities including research into latest threat sources, malware, attack/defence methodologies and techniques. * Operate, manage and maintain security tools and platforms including, but not limited to endpoint security software, Splunk Security Information and Event Management system (SIEM), email security tools, internal and external firewalls and VPN and remote access. * Develop and maintain Use Cases for detecting and responding to potential security incidents, including configuration of alerts and responses to indicators of compromise (IoCs). * Use of Splunk SIEM to proactively monitor security events/alerts on a daily basis and respond to potential and actual threats quickly. * Perform regular vulnerability scans across university assets to discover and mitigate known vulnerabilities and work with technical owners to eliminate discovered vulnerabilities. * Respond to security incidents such as network intrusions, compromised accounts, etc., quickly and prevent recurrence through root cause analysis. * Work with IT Operations teams to resolve issues and questions related to information security. * Work with and coach junior members of the security operations team and assist in providing education, training, and coaching where appropriate. |
| Security Assessment | * Coordinate or execute penetration testing of university systems, including infrastructure and applications. * Conduct risk assessments associated with third party vendor service providers. * Provide security advice on security architecture and controls as part of any systems acquisition/development projects. * Participate in the Change Advisory Board (CAB) to review and approve proposed changes to systems in the absence of the Chief Information Security Officer. |
| Security Awareness Training | * Assist with the development and delivery of security training programs for general University staff, as well as targeted training for specific user groups. * Plan and execute periodic phishing simulations to deliver “just in time” learning to staff. |
| Continuous Improvement | * Feedback learnings from security operations and security assessments into the continuous improvement of the University’s security posture and resilience capabilities. * Contribute to the development and enhancement of the cyber security strategy/roadmap. * Participate in the information risk management framework through review of policies, coordination of compliance audits, and implementation of treatment plans. |
| Develop and Maintain Personal and Professional Skills | * Maintain current knowledge of information technology and best practices in the delivery of IT services, especially pertaining to cyber security. * Participate in development courses and seminars as appropriate. |
| Stakeholder Engagement and communications | * Establish and maintain strong and effective professional relationships and networks with team members across the ITDS branch and wider University. * Contribute positively to the team environment and supporting the goals of ITDS and the University. * Actively share expertise and knowledge related to continuous improvement and IT governance with ITDS branch and wider University staff. * Design and deliver stakeholder engagement activities and communications in conjunction with relevant stakeholders. |
| Other reasonable duties commensurate with classification level. | |

|  |
| --- |
| **PEOPLE MANAGEMENT RESPONSIBILITIES** |
| * N/A |

|  |
| --- |
| **CAPABILITIES AND BEHAVIOURS** |
| Use the [Capability Dictionary](https://www.adelaide.edu.au/hr/ua/media/1605/rec-core-capability-dictionary.pdf) to identify the capabilities associated with the classification of this position. Staff are required to read and understand the capabilities and associated behaviours that align with the classification of this position. |

|  |
| --- |
| **UNIVERSITY EXPECTATIONS** |
| Staff are required to read, understand, and comply with all University policies, procedures, and reasonable direction, whilst demonstrating professional workplace behaviours in accordance with the University’s Code of Conduct |

|  |
| --- |
| **STAFF VALUES AND BEHAVIOUR FRAMEWORK** |
| Our culture is one that welcomes all and embraces diversity consistent with our [Staff Values and Behaviour Framework](https://www.adelaide.edu.au/hr/organisational-development/university-values) and our Values of integrity, respect, collegiality, excellence and discovery. We firmly believe that our people are our most valuable asset, so we work to grow and diversify the skills, knowledge, and capability of all our staff. |

|  |
| --- |
| **SELECTION CRITERIA** |
| **Knowledge and Experience:**   1. Demonstrated understanding of IT infrastructure technologies including IP networking, client/server operating systems (Windows, Unix, and MacOS), database systems, messaging systems, and security tools such as firewalls, endpoint security protection, and Security Information and Event Management systems (SIEMs). 2. Extensive experience and demonstrated working knowledge of information security threats and preventive/detective technologies and techniques. 3. Ability to write program code in a scripting language such as Python and JavaScript is a plus. 4. Demonstrated ability to communicate, present and influence credibly and effectively at all levels of the organisation, including senior executive. 5. Demonstrated ability to work independently and with initiative, set priorities and balance the demands of a complex working environment. 6. Proven track record in providing insightful advice and guidance to a broad range of stakeholders up to and including senior executives.6. Demonstrated ability to promote the organisational values of integrity, respect, collegiality, excellence and discovery, and a commitment to positively comply with the associated behaviour expectations.   **Qualification/s:**   * Postgraduate qualifications or progress towards postgraduate qualifications in computer science or related discipline and extensive relevant experience; or * An equivalent combination extensive experience and/or education/training. * Relevant industry technical security certificates such as OSCP, OSCE, CISSP, GIAC and vendor qualifications by Microsoft, Cisco, etc. (desirable) |