Position Description - Senior Security Operations Engineer

Updated 12/06/2024

POSITION DETAILS	
Portfolio	**Corporate Services**
Organisational Unit	**Information and Digital Services (IDS)**
Supervisor	**Deputy Chief Information Security officer**
Classification	**Higher Education Officer Level 8**
Employment Type	**Continuing, Full Time**

POSITION SUMMARY

Under broad direction, the role is responsible for implementing cyber security initiatives across the University and carrying out and implementing specialised cyber security controls, services, and activities.

The role is also responsible for supporting the research and evaluation of procedural and technical controls and solutions that can be applied to provide security to the University's IT networks and systems.

The role works closely with other practitioners and teams to ensure the ongoing security and effectiveness of the University's network and system assets, and the stable and continuous operation of the University's mission-critical systems and applications.

UNIVERSITY EXPECTATIONS AND VALUES

All staff at Flinders are responsible for understanding their obligations and responsibilities as set out in the University's code of conduct and are expected to:

- demonstrate commitment to the University's values of Integrity, Courage, Innovation, Excellence and the underlying ethos of being Student Centred;
- contribute to the efficient and effective functioning of the team or work unit in order to meet the University's objectives. This includes demonstrating appropriate and professional workplace behaviours, providing assistance to team members if required and undertaking other key responsibilities or activities as directed by one's supervisor;
- promote and support an inclusive workplace culture which values diversity and embraces the principles of equal opportunity;
- perform their responsibilities in a manner which reflects and responds to continuous improvement; and
- familiarise themselves and comply with the University's *Work Health and Safety, Injury Management and Equal Opportunity* policies.

This role requires Australian citizenship and a current Defence security clearance of Baseline or above, or the ability and willingness to be processed for such a clearance.

A National Police Certificate which is satisfactory to the University will be required by Flinders University before the successful applicant can commence in this position.

An up to date COVID-19 vaccination may be required as a condition of employment, in accordance with the Flinders University COVID-19 Vaccination Policy (2022). If required, any offer of employment will be subject to the successful candidate presenting their COVID-19 Digital Certificate as evidence of vaccination or showing evidence of a valid medical exemption, where relevant.

KEY POSITION RESPONSIBILITIES

The key position responsibilities include:

Technical Management & Support

1. Configuring, deploying and maintaining new and existing security platforms, including email filtering, firewall, intrusion prevention/detection systems, and VPN and host protection systems.
2. Managing the ongoing application of the IDS risk register, identifying and ensuring the management of key risks that may impact on the security of the University's systems and networks.
3. Maintaining and implementing effective security policy for new and existing security platforms and tools, to ensure a positive security posture and sustainable IT services environment for the University.
4. Monitoring, responding to, and resolving cybersecurity incidents and trouble tickets assigned to the team for security resolution.
5. Responding to technical investigations of cybersecurity events and incidents, deploying effective mitigations for cyber threats and incidents, and documenting findings in incident reports.
6. Supporting the University as its nominated Defence Industry Security Program (DISP) Officer, which includes maintaining DISP artifacts and managing the University's implementation of DISP processes and compliance.

Technical Vision & Roadmap

7. Supporting with identifying technological trends and developing reports as necessary to keep IDS management apprised of information security threats and planned equipment or software changes that could impact system and network security and availability.
8. Developing and implementing security policies and procedures and ensuring understanding and compliance by other technical staff. Developing and modifying guidelines, processes, systems and metrics in pursuit of best practice and to establish a culture of continuous improvement.

Technical Knowledge & Excellence

9. Providing advice to projects and undertaking security reviews of new cloud-based systems and platforms intended to be used by the University, in order to ensure the levels of protection appropriate to their use.
10. Providing support on security matters relating to disaster recovery and business continuity, ensuring that disaster recovery plans and business continuity plans appropriately address security requirements in maintaining the provision of services.
11. Conducting both formal and informal market scanning and benchmarking activities to be aware of emerging market offerings and trends.
12. Periodically participating in knowledge building activities and events to be aware of latest/best practices related to the role and to keep skills and knowledge up to date.

Risk, Governance & Ways of Working

13. Supporting and maintaining an agile based way of working to manage, refine, and prioritise the activity backlog based on relevant customer and IDS priorities.
14. Identifying, managing and mitigating risks related to the activities being undertaken by the role in line with IDS and Flinders University policies and procedures.
15. Ensuring compliance with all relevant IDS and Flinders University policies and procedures.

Other Responsibilities

16. Any other responsibilities in line with the level of the role as assigned by the Supervisor and/or the University.

KEY POSITION CAPABILITIES

- Appropriate tertiary qualification in Information Technology or relevant technical area, and / or equivalent relevant experience in an IT environment.
- High level strategic thinking, planning and analytical skills to support outcomes and meet the University's strategic goals.
- High level interpersonal and relationship management skills.
- Broad experience in building and managing customer relationships and expectations.
- Broad experience in agile ways of working including exposure to scaled agile methodologies and/or collaborating and delivering through a matrix structure.
- High level self-improvement and growth mindset/approach to the role and as part of a wider team.
- High level interpersonal influence and demonstrated ability to negotiate and communicate effectively with staff and customers across a diverse organisation particularly during the design, management and implementation of customer solutions.
- An industry recognized security certification, for example CISSP, CISM, CISA, SSCP, CEH, CRISC, GIAC or equivalent is advantageous.
- High level experience in performing system administration and/or network management roles at journeyman or higher practitioner levels.
- Ability to resolve cybersecurity events and problems at Level 2 or Level 2+ competency.
- A broad understanding of IT security in the context of higher education environment, with particular reference to systems, networks and applications that are used and how these relate to attaining a good cybersecurity posture.
- Higher education experience advantageous.