Cyber Security Specialist

ASX Position Description

ASX "All Roles Flexible"

ASX offers mutually beneficial flexible working arrangements.
We recognise that employees need to balance work and personal lives.

ASX Opportunity Snapshot	
Role:	Cyber Security Specialist
Reports to:	Cyber Security Manager - Architecture
People Management:	N/A
Budget:	N/A
Team:	Technology
Date:	April 2019
Location:	Sydney, NSW
Flexible Role:	Yes

What's On Offer

Technology Security is a critical component of ASX's enterprise risk management framework and is viewed as an enabler for ASX staff and customers. This specialist role has been created to work within the current cyber security team and will primarily be responsible for providing security consulting to projects and other areas of the business, assessing the current security environment, recommending and designing system / network / application security architecture aligned with threat levels and risk appetite, coordinating the vulnerability management program (e.g. security testing, patch management, internal scanning), maintaining the security registers (e.g. issues, incidents and exceptions) developing, investigating potential security incidents and maintaining security policies and standards. It is a multifaceted security 'hands on' role working in a small team of dedicated security professionals to enhance the security environment and improve operational efficiency.

What you'll do:

- Provision of security consulting and advice to various areas of the organisation, ensuring that new initiatives are aligned with the ASX security framework
- Design of network / system / application security architectures and controls, including for externally managed environments
- Security design implementation advice
- Performing overall security risk assessments, particularly in relation to security design
- Evaluation, assessment and recommendation of security tools and products
- Liaison with the Technology Infrastructure (and other internal teams) to facilitate appropriate security outcomes
- Management of the vulnerability management processes, including security testing and scanning and maintenance of security issues, incidents and exceptions registers
- Assist in management of the security documentation suite, including the development of policies, procedures and standards

- Assist in further developing a practical security architecture and compliance framework for protects and new initiatives
- Assist in the performance of data and threat risk assessments
- Assist in the development of security metrics and KPI's
- Liaise with internal and external assurance functions as required
- Potentially conducting investigations (e.g. root cause analysis) and trend analysis of security issues and events as required
- Assist in the preparation of management and Board reporting as required.

What you've done:

- Extensive experience in the design of secure architecture
- Experience in privilege access management, identity and access management and PKI solutions
- Exposure to HSM implementations
- Exposure to big data platforms
- Exposure to security design as it relates to 'X'aaS services (e.g. Office 365, Atlassian, Salesforce) and (in general) to externally managed environments
- Implemented design frameworks
- Performed security risk assessments
- Exposure to industry standard security frameworks and good practice guidelines (e.g. NIST, ASD, CIS)
- Process risk and control mapping techniques
- Familiarity with operating systems including Windows, Linux, VMS; and application solution such as, Active Directory, Exchange, SQL, Skype, security systems such as firewalls, load balancers, anti malware, patching.
- Exposure to data leakage prevention controls
- Development of security related documentation (policies, procedures, standards)
- Exposure to the performance of penetration testing and vulnerability scanning
- Exposure to cloud based technologies and associated security controls

And if you've got some of this, even better:

- Exposure to container platforms (e.g. Kubernetes) and cloud based technologies (e.g. Google cloud)
- Worked in a security operations centre environment
- IT degree with a focus on IT Security
- Understanding of current Australian regulatory environment (as it relates to financial services / clearing and settlement providers) and related implications to identity management and security/audit compliance
- Post graduate security qualification (e.g. CISSP, Cloud)

What you need to enjoy and be good at for this role:

- Influencing and communicating with all levels of management and external stakeholders
- Strong control awareness in an environment where this is no room for compromising on process and control

- Desire to work analytically to identify and resolve operational security issues
- Enjoy working in a collaborative environment to implement and maintain best practice security protocols
- Ability to take a broad view of his/her position and take initiative to communicate, interact and cooperate with others
- Be aligned with ASX values – “Be Open”, “Be Trustworthy”, “Be Original”, “Be the example”