Australian Red Cross
THE POWER OF HUMANITY

POSITION DESCRIPTION – TEAM MEMBER

Position Title	IT Security Engineer	Department	Information Technology
Location	Sydney or Melbourne	Direct/Indirect Reports	
Reports to	Head of ICT Operations	Date Revised	December 2018
Industrial Instrument	Social Home Care and Disability Services Award		
Job Grade	Job Grade 6		

■ Position Summary

The IT Security Engineer performs three core functions for the enterprise. The first is the day-to-day operations of the in-place security solutions (Firewall, IPS, Proxy, Anti-malware, SIEM, DLP, IVA, etc.), the second is the monitoring, identification, investigation and resolution of exceptions/ incidents detected by/ identified against these systems, and the third is executing security scans and assessments of the enterprise IT infrastructure, systems, applications and data. This role is required to coordinate and work very closely with Information Security, IT Customer Services, Technical Services and Enterprise Business Applications teams to identify, prioritize and implement required security controls.

Other tasks assigned to this role may include involvement in the implementation of new security solutions, participation in the creation and or maintenance of policies, procedure, standards, baselines and guidelines as well as periodic reporting of vulnerabilities, security gaps and the mitigation action plans.

The IT Security Engineer is expected to be fully aware of the enterprise's security goals as established by its stated policies, procedures and guidelines and to actively work towards upholding those goals. This role is a member of ICT Operations team and may at times assist with other information security governance and management activities as required.

■ Position Responsibilities

Key Responsibilities

Strategy & Planning

- Participate in the planning and design of enterprise security architecture
- Participate in the creation of enterprise security documents (policies, procedures, standards, baselines and guidelines)
- Participate in the planning and design of an enterprise Business Continuity Plan and Disaster Recovery Plan
- Participate in the enterprise risk assessment, prioritization and remediation planning

Acquisition & Deployment

- Perform the deployment, integration and initial configuration of new security solutions and of any enhancements to existing security solutions in accordance with leading practices and enterprise's security requirements.
- Maintain up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the latest attacks and threat vectors.
- Recommend additional security solutions or enhancements to existing security solutions to improve overall enterprise security.

Operational Management

- Maintain up-to-date baselines for the secure configuration and operations of in-place devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.).
- Maintain operational configurations of in-place security solutions as per the established baselines.
- Monitor and review in-place security solutions for effective, efficient and appropriate operations.
- Monitor alerts, logs and exception reports generated by in-place security devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.). Interpret the implications of such alerts or exception reports, escalate security incidents and assist in devising plans for appropriate resolution.
- Execute security scans and assessments of the enterprise IT infrastructure, systems, applications and data.
- Escalate problems and assist with incident response.
- Contribute to analysis/ investigation of problematic activities to discover and resolve issue.
- Assist in security monitoring, tracking, reporting and management.

■ Position Selection Criteria

Technical Competencies

- Significant experience in IT Security/ Cyber Security service delivery essential.
- Highly developed analytical and technical problem solving skills.
- Implementation, configuration, operation and monitoring of UTM firewalls, antivirus systems, vulnerability management solutions, SIEM solutions and DLP solutions.
- Experience developing technical standards, baselines and guidelines aligned with NIST/ CIS and OEM recommendations.
- Experience working with cloud environments (AWS, Azure, Office 365).
- Experience with Fortigate & Palo Alto Security devices
- Experience with writing scripts in one or more scripting languages (PowerShell preferred).
- Experience in administering highly available IT security systems/ solutions.
- Experience with large, multi-site technical environments.
- A good understating of IT security architecture principles and concepts.
- Exposure to project management and IT service delivery management methodologies/ practices.
- Exposure to IT security governance and risk management frameworks (ISO27001/ COBIT/ ITIL).

Qualifications/Licenses

- Relevant Tertiary Qualification required.
- One or more industry/ OEM certifications is essential (in network security such as PCNSA/PCNSE, FCNSA, cloud platform certifications with a security focus, MCSA/ MCSE – Cloud Platforms with a security focus, vulnerability management solutions, Advanced Threat Protection technologies or SIEM technologies).
- One or more information security certifications will be a definite advantage (CISSP/ CCSP, CISM/CISA, GIAC/ OSCP, CompTIA Security+).

Behavioural Capabilities

- **Personal effectiveness | Being culturally competent |** Demonstrated understanding and appreciation of cultural differences and diversity in the workplace. Always displaying respect and courtesy to others and acknowledges cultural heritages and varying perspectives of team members.

- **Team effectiveness | Managing performance |** Demonstrated capability to take ownership of work and use initiative to deliver results. Accountable for own performance and ability to set clearly defined objectives for achievement.
- **Team effectiveness | Communicating |** Demonstrated capability to communicate clearly and concisely ensuring messages are understood. Ability to express ideas clearly, listen effectively and provide feedback constructively.
- **Organisational effectiveness | Innovating and improving |** Demonstrated ability to identify and raise issues regarding ineffective work processes and take initiative to make improvements.
- **Organisational effectiveness |Managing risk |** Demonstrated ability to work within guidelines, policies and procedures. Awareness of risks involved in an individual's role and works toward minimising their impact.

■ General Conditions

All Red Cross staff and volunteers are required to:

- Adhere to the 7 fundamental principles of Red Cross:

  Humanity | Impartiality | Neutrality | Independence | Voluntary Service | Unity | Universality
- Act at all times in accordance with the Australian Red Cross Ethical Framework and Child Protection Code of Conduct
- Demonstrate skill, knowledge and behaviour to work with Aboriginal and Torres Strait Islander people in a culturally respectful way
- Comply with the Work Health and Safety management system
- Undertake a police check prior to commencement and every 3 years thereafter. Police check renewals may be required earlier than 5 years in order to comply with specific contractual or legislative requirements
- Support a child safe organisation by undertaking screening for suitability to work with children, youth and vulnerable people and to comply with relevant state/territory legislative requirements
- Assist the organisation on occasion, in times of national, state or local emergencies or major disasters