Job Description

25 September 25

Cyber Security Engineer - Security Operations
SBS Technology

Reports to: Manager, Information Security

Direct reports to this position: N/A

SBS Values, Vision and Purpose

The Cyber Security Engineer – Security Operations is responsible for undertaking their work in a way that reflects SBS's Charter, Vision and Values and complies with relevant SBS policies, procedures and practices. At SBS, we expect you to be audience obsessed, be bold and brave, embrace difference, participate fully and ensure that we look out for one another. We are all working together to fulfil SBS's purpose and create a more cohesive society.

Division Purpose – Technology

SBS Technology *can be thought of as the 'engine room' of SBS. Our primary role is to enable and support the production, distribution, and transmission of content across television, radio, and online platforms. Our teams achieve this by working collaboratively to design innovative solutions and deliver end-to-end services for our business stakeholders.*

Role Purpose

The Cyber Security Engineer – Security Operations plays a key role in the design, deployment, automation, and ongoing management of security technologies across the organisation. This role will have you working across Elasticsearch SIEM, CrowdStrike EDR, Microsoft 365/EntraID security, AWS cloud security, and a range of interesting security uplift projects slated for now and the future.

The successful candidate will bring experience in supporting multiple cyber solutions concurrently, along with excellent communication skills and a keen interest in working across all facets of cyber security.

In addition to project delivery, this role includes hands-on involvement in security operations and alert

response with participation in an emergency response on-call roster.

If you thrive on variety, love problem solving, and are keen to be a part of a small team invested in the cyber resilience of Australia's most trusted multilingual broadcaster, then this is your chance to make a difference.

Main Responsibilities

Main tasks of the role

- Manage and deploy Elasticsearch SIEM components, Elastic Agent and security integrations including creating and tuning security detections, alerts, and dashboards.
- Manage, deploy and monitor CrowdStrike Falcon EDR, ensuring optimal security posture across endpoints.
- Manage and secure Microsoft 365, EntraID security features, including Defender for Office 365 and Conditional Access Policies.
- Take the lead in the design and deployment of cyber uplift projects across centralised endpoint management and identity and access management.
- Ensure Active Directory security is maintained and benchmarked against best practice initiatives.
- Monitor AWS security services such as GuardDuty, Security Hub, and CloudTrail for suspicious activity.
- Monitor and respond to security alerts and incidents.
- Support security risk assessments and contribute to vulnerability management efforts.
- Maintain and update security software documentation, incident playbooks, and response procedures.
- Leverage PowerShell, Python and Power Automate to streamline security response workflows.
- Act as a key technical resource for security improvements across the organisation.

Minimum Requirements:

- Experience in a similar Engineering role with an analytical background.
- Proficiency in managing SIEM components (preferably Elasticsearch and Elastic Stack)
- Knowledge of security frameworks such as NIST, ASD Essential 8, and MITRE ATT&CK.
- Ability to work and troubleshoot independently and contribute to security automation projects.

Further Desirable Requirements:

- Certification in Elasticsearch (Elastic Certified Engineer or Analyst).
- SANS GCFA (Certified Forensic Analyst) or similar security certification.
- Experience with network security and firewall management.
- Experience working in a Security Operations Centre (SOC) environment.

Key Capability		
Capability	**Level**	**Behaviour**

Coaching (People Leader Capability)	Operation	• Seeks feedback from the business to drive coaching competence • Ensures leaders exhibit coaching values and behaviours • Strikes a balance between skills-based and behavioural coaching • Prioritises resources to support a coaching culture • Drives a coaching style of leadership across the business
Collaboration	Operation	• Encourages collaboration (sharing of responsibility and information) across the business • Encourages shared goals by promoting joint responsibility • Ensures expert knowledge is continuously enhanced and shared across the business • Acts to promote respect, helpfulness and co-operation across the business • Publicly credits individuals across the business who have performed with excellence
Customer Focus	Operation	• Grasps a customer/client's perspective, acting as a trusted advisor • Analyses the degree of customer and/or client penetration • Keeps abreast of competitor products and services • Measures the impact of customer/client service across the business • Analyses the degree of customer/client satisfaction • Encourages a long-term commitment to customer/client needs • Advocates the principles of customer/client relationship management via policies • and/or procedures
Innovation	Operation	• Scans the environment for new ideas and innovative opportunities to benefit business • Takes calculated risks to get a business advantage • Implements modifications to processes and procedures to improve current performance • Generates original solutions that facilitate the achievement of business goals • Proposes creative and functional solutions to benefit the business • Supports the development of creative business strategies • Manages the implementation of creative business strategies • Recognises and rewards creativity and innovation
Organisational Awareness	Operation	• Considers how functions within the business work together • Uses SBS's structure, procedures and/or systems to achieve objectives • Understands the key drivers that impact the business • Identifies potential risks, and/or opportunities across the business

		• Considers the impact of potential risks, and/or opportunities across the business • Uses financial reporting information to inform business decision making
Results Focus	Operation	• Strives to improve business performance and maximise value • Ensures managers seek alternative possibilities when faced with obstacles • Streamlines projects and functions to ensure efficient outcomes • Ensures business initiatives are completed within designated timeframes • Is tenacious in achieving results that drive the business forward • Strives to meet financial objectives

Workplace Health & Safety

In relation to Work Health & Safety, you must comply with your safety responsibilities as detailed in relevant Acts, Regulations, Standards, Codes of Practice and the SBS Safety Management System (SMS)

All workers are required to:

- Take reasonable care for own safety and safety of others
- Cooperate with policies and procedures and directions from management with regards to health and safety
- Where hazards are identified, report them to line manager and take corrective action where able
- Report all work related incidents to line manager within 24 hours of occurrence
- Ensure workers, visitors and clients are:
    - made aware of their WH&S responsibilities
    - have received adequate safety induction and other WH&S information, instruction and training to enable them to conduct their work safely
    - follow safe work practices