Job Description

6 August 25

Senior Cyber Security Engineer
SBS Technology

Reports to: Manager, Information Security

At SBS, we embrace difference, and we welcome applications from people of all backgrounds.

We also acknowledge the unique contribution that Aboriginal and Torres Strait Islander peoples make to our society and our workplace through their enduring and continued connection to land, sea, sky and community.

About Us

SBS is one of the world's most unique and innovative media organisations, producing trusted, meaningful, and engaging content that exists for all Australians to inspire, support and celebrate the diversity of our multicultural society.

Our purpose, for the last 50 years, has reflected and explored the evolving diversity of Australia, investing in initiatives to deepen its connections with communities, sharing their stories and giving a voice to those often unheard, with the aim of increasing understanding and respect of the differences that make up Australia.

SBS is a truly distinctive network, showcasing multicultural, multilingual and First Nations stories otherwise untold in the Australian media.

The Department

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 Senior Cyber Security Engineer plays a key role in the design, deployment, automation, and ongoing management of security technologies across the organisation. The role has a strong technical focus, particularly in Elasticsearch, CrowdStrike EDR, Forensic tools, Microsoft 365 security, AWS security and security automation.

The successful candidate will bring proven expertise in the design, implementation, and support of cyber security solutions, along with excellent communication and relationship-building skills to work effectively across business and technical teams.

In addition to project delivery, this role includes hands-on involvement in security operations, including alert monitoring, incident response, and participation in an on-call roster.

This is a senior position that requires deep technical acumen and the ability to collaborate across departments to uplift and maintain the organisation's security maturity at scale. You will be involved in all facets of security roles and responsibilities where one day is rarely the same as the next.

Main Responsibilities

Main tasks of the role

1. **SIEM & Threat Detection**
   - Manage and deploy Elasticsearch SIEM components, including Elastic Agent and security integrations.
   - Create and tune security detections, alerts, and dashboards within Kibana.
   - Integrate security log sources (e.g., AWS, Microsoft 365, CrowdStrike, Velociraptor) into the SIEM for continuous monitoring.
   - Develop automation scripts to enrich security data and improve threat intelligence correlation.
   - Conduct proactive threat hunting using SIEM and EDR systems.

2. **Architecture and Design**
   - Actively participate in the selection, design and configuration of new security tools
   - Research and configure Blue Team security uplift responses to active testing.
   - Act as a key technical resource for security improvements across the organisation.

3. **Endpoint Detection and Response**
   - Manage and deploy CrowdStrike Falcon EDR, ensuring optimal security posture across endpoints.
   - Monitor, analyse, and respond to CrowdStrike security alerts, identifying and mitigating potential threats.
   - Configure and fine-tune CrowdStrike policies to enhance detection and prevention capabilities.
   - Leverage CrowdStrike APIs to automate detection, response, and forensic investigations.
   - Develop and implement Falcon Real Time Response (RTR) scripts to automate remediation.

4. **Microsoft 365, EntraID and Active Directory Security**
   - Manage and secure Microsoft 365, EntraID security features, including Defender for Office 365 and Conditional Access Policies.
   - Ensure Active Directory security is maintained and benchmarked against best practice initiatives.
   - Monitor security compliance within Microsoft cloud environments.

5. **AWS & Cloud Security Management**
   - Monitor AWS security services such as GuardDuty, Security Hub, and CloudTrail for suspicious activity.
   - Develop AWS security automation for monitoring, alerting, and response.
   - Implement and manage AWS IAM policies to enforce least privilege access.
   - Ensure AWS logging and monitoring are correctly configured to feed into SIEM and security tools.

6. **Security Compliance & Continuous Improvement**
   - Support security risk assessments and contribute to vulnerability management efforts.
   - Assist in audit and compliance activities, ensuring adherence to security policies and regulatory requirements.
   - Maintain and update security documentation, incident playbooks, and response procedures.

7. **Automation & Security Engineering**
   - Leverage PowerShell, Python and Power Automate to streamline security response workflows.
   - Automate security event triage and remediation using SOAR methodologies.

8. **Technical Guidance and Support**
   - Provide technical guidance, and day-to-day support to Cyber Engineers and Cyber Analysts, where required, to enhance their capabilities in security operations, incident response, vulnerability management, and secure systems design.
   - Demonstrate expertise through knowledge sharing and practical demonstrations of tools, techniques, and best practices in areas such as SIEM configuration, threat identification, and system fortification.
   - Facilitate upskilling in emerging cyber technologies, frameworks, and methodologies to ensure the team's proficiency in evolving threats and regulatory requirements.
   - Act as a trusted escalation point for complex technical issues, providing expert input and encouraging critical thinking and solution-oriented approaches among the team.

Minimum Requirements:

- 5+ years in a similar Engineering role and proven experience across cyber security roles.
- Proficiency in managing Elasticsearch and Elastic Stack components is required for this role (Elastic Agent, SIEM integrations, Kibana).
- Experience in researching and implementing proactive defensive initiatives in direct response to new or targeted attack techniques seen across the treat landscape.
- Proven experience designing, managing and supporting security uplift projects from inception to completion involving coordination across multiple departments.
- Expertise in managing and deploying CrowdStrike Falcon EDR (policy tuning, threat response, automation).
- Experience in developing automation using CrowdStrike APIs, RTR scripting, and Falcon platform tools.
- Proficiency in securing and monitoring Active Directory.
- Deep understanding of AWS security services (GuardDuty, Security Hub, IAM, CloudTrail, etc.).
- Experience managing security in Microsoft 365, EntraID and Exchange Online environments.
- Knowledge of security frameworks such as NIST, ASD Essential 8, and MITRE ATT&CK.
- Ability to build security detections, alerts, and automation in SIEM solutions.
- Ability to work 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.
- Strong scripting and automation skills using Python, BASH, and PowerShell.
- Experience with Power Automate for security workflow automation.
- Experience with network security and firewall management.
- Experience working in a Security Operations Centre (SOC) environment.

Key relationships with other roles and external stakeholders

- Build and maintain a strong network of contacts and relationships across the Australian TV, digital media and technology vendor communities, both locally and internationally where appropriate.
- Represent the interests of SBS within appropriate forums and liaise with other stakeholders to ensure that the strategies and services reflect the operational needs and SBS Charter e.g., Privacy and Data Safety i.e., Information Governance, Legal, Risk, Privacy.

Some of the reasons to consider working with us

- The people! We truly celebrate and welcome difference at SBS and encourage everyone to bring their whole self to work & you'll be part of one of the most inclusive companies in Australia!
- The culture and the engagement of our workforce! 93% of our employees have stated that they are proud to work for SBS!
- We offer a range of benefits from, health care checks, salary packaging, Employee Assistance Programme, flexible work arrangements and discounted gym membership nationally with Fitness Pass.
- We're agile and innovative in the way we work, as well as being a trusted and established brand. At SBS we have been broadcasting for over 50 years and our future is packed with many more exciting developments!
- We also love to promote from within! We have allocated training funds to do just that and help bridge the gaps when moving from role to role.

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