Position Description

Job title:	Security Operations and Engineering Manager
Department:	Security
Work type:	Full time
Reports To:	Chief Information Security Officer
Position Reports:	3
Position Contact:	Chief Information Security Officer

About the organisation

.au Domain Administration (auDA) is the administrator of the .au domain name system (DNS), which is Australian critical infrastructure relied on by internet users in Australia and around the world. We are a not-for-profit endorsed by the Federal Government.

Our purpose is to administer a trusted .au domain for the benefit of all Australians and champion an open, free, secure and global internet.

We support the needs of Australian internet users by:

- Delivering a stable, secure and reliable .au DNS
- Implementing .au policy rules that are transparent, responsive and efficient
- Investing in the Australian internet ecosystem to improve the utility of the .au domain.

We also participate in global internet governance processes. Through our work, we strive to uphold the multi-stakeholder model of internet governance and the social and economic benefits that flow from it.

Further information about auDA is available at www.auda.org.au.

Our values

Leadership

We are committed to communicating openly, and adding value to our multistakeholder community, locally, regionally and globally

Collaboration

We work together as one auDA in the service of Australian, regional and global internet users

Accountability

We honour our commitments, are responsible for our decisions, actions and performance, and deliver excellence

Curiosity

We seek to grow our knowledge, including of emerging practices, be adaptive and improve our understanding of our stakeholders and their viewpoints

Role purpose

The Security Operations and Engineering Manager plays a critical role in strengthening auDA's cybersecurity posture and ensuring the ongoing resilience of our information assets, services and the .au domain name system. This position is responsible for leading the technical security functions and team at auDA including the security operations and security engineering practices. The manager will lead efforts to deliver, maintain and operate security tools, infrastructure and operational processes that help to protect auDA. They will own and coordinate technical incident response activities and plans across security and technology.

This role will contribute significantly to auDA by safeguarding critical infrastructure, sensitive data, and maintaining the trust of its stakeholders. By proactively defending and safeguarding against threats, managing vulnerabilities, and building a positive control environment, the Security Operations and Engineering Manager will help prevent security incidents and protect auDA's reputation. The role will report directly to the Chief Information Security Officer and will be instrumental in translating security into actionable strategies, supporting auDA's mission to operate a secure and stable domain name system for all Australians. This role is pivotal to auDA’s objective to provide a cyber resilient .au that builds trust, enables innovation and builds the capabilities needed into the future.

This role will suit a candidate with a strong background in security operations and engineering, incident response, and team leadership, possessing excellent communication and stakeholder management skills. The ideal candidate will be a proactive, detail-oriented individual with the ability to communicate complex technical concepts effectively to both technical and non-technical audiences. They should demonstrate a proven track record in leading security operations and engineering teams, leading security incident response, managing stakeholder relationships and driving continuous improvement in a dynamic environment.

Key accountabilities

As the Security Operations and Engineering Manager, you will lead our technical security initiatives, focusing on both proactive defence and strategic engineering. Your core responsibilities include:

Security Operations

- Lead Threat Detection and Response: Collaborate with our Managed SOC provider to ensure timely and effective threat detection, automation, and response
- Enhance Defensive Posture: Drive regular threat hunting, penetration testing, and red teaming exercises. Manage threat intelligence to inform and improve our defences
- Oversee Vulnerability Management: Own the end-to-end vulnerability and patch management process, from asset coverage and prioritization to reporting and remediation
- Ensure Continuous Monitoring: Monitor key operational controls and security events to maintain a strong security posture
- Manage the Team: Lead and coach a small team of security professionals.

Security Engineering

- Design and Implement Security Controls: Define technical security requirements and design solutions for new projects, as well as implement and maintain key controls and systems such as EDR, IAM, Logging, Cloud Security, and Application Security
- Drive Continuous Improvement: Develop and manage a program to continuously improve our security controls and technical readiness
- Enable Detection Engineering: Facilitate the detection engineering lifecycle together with our Managed SOC, from threat modelling to creating and refining detection logic
- Act as a Subject Matter Expert: Provide technical security expertise during product selection and systems design.

Incident Response

- Lead Incident Management: Serve as the lead incident manager, coordinating and directing security and technology incident response activities
- Manage the IR Lifecycle: Create and maintain incident response plans, playbooks and lead post-incident reviews, root cause analysis, and digital forensics
- Ensure Team Preparedness: Facilitate regular training and drills to keep the team "match-fit" and ready to respond.

Other responsibilities

- Provide regular operational security reporting on performance and key cyber metrics
- Provide information to support control assurance activities and audits as required
- Support delivery on auDA's Cyber Security Strategy and associated Cyber Security Program
- Other activities as directed by the Chief Information Security Officer and Chief Operating Officer to support the delivery of auDA's Strategy and the Security strategic goals.

Key selection criteria

Security Operations and Leadership

- Proven Leadership: Extensive experience leading and mentoring high-performing security teams, fostering a culture of continuous improvement
- Threat & Vulnerability Management: Expertise in managing and optimizing vulnerability management programs and a demonstrated ability in threat hunting, modelling, and intelligence
- Incident Response: Hands-on experience creating and executing incident response plans, leading end-to-end incident response activities, and performing post-incident reviews
- Vendor Management: Experience collaborating with external security providers and Managed Security Service Providers to achieve defined security outcomes
- SIEM/SOAR Expertise: Proven ownership and operational experience managing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) capabilities.

Security Engineering

- Technical Control Implementation: Demonstrated experience implementing and maintaining technical security controls in alignment with recognized industry standards (e.g. ISO 27002, NIST 800-53 & ACSC's Essential Eight)
- Solution Design & Implementation: A strong background in designing, implementing, and reviewing solutions to achieve security outcomes and mitigate risks effectively
- Threat Modelling: Experience performing threat modelling to identify and address security threats proactively
- Security Program: The ability to drive and implement strategic improvements in security controls and processes.

Interpersonal & Communication Skills

- Stakeholder Engagement: Excellent communication skills with a proven ability to engage, influence, and provide expert security guidance to a diverse range of internal and external stakeholders
- Problem-Solving: Strong analytical and problem-solving abilities, coupled with a proactive, detail-oriented approach to cybersecurity challenges
- Collaborative Mindset: A track record of fostering a security-conscious culture and building strong relationships across an organisation.

Additional Requirements

- Organisational Skills: Strong planning and organisational skills, with the ability to manage multiple priorities and projects concurrently
- Work Ethic: A proactive, self-motivated attitude with a proven ability to lead by example and inspire team members
- Flexibility: Willingness to work occasional hours outside of normal business hours and undertake domestic or international travel only as required.

Qualifications and experience

- A minimum of 5 years' experience in a dedicated Security Operations Manager role
- At least 10 years of experience in security related roles
- Background in a regulated industry, such as financial services or critical infrastructure, is advantageous
- A degree in a technology or security related field is advantageous
- Experience working in organisations of varying sizes will be highly regarded.

Important information

Background checks

A National Police Check, Right to Work and bankruptcy will be conducted as part of the recruitment process. An *AusCheck Critical Infrastructure Background Check* will need to be conducted and there may be a need to obtain Government security clearances as part of this role. Where applicable, international background checks may also be required.

Privacy collection information

.au Domain Administration Limited ACN 079 009 340 collects your personal information for the purpose of assessing and responding to your application. All personal information is collected in accordance with the *Privacy Act 1998* (Cth) and our Privacy Policy.

We, or our third-party tools or platforms, may disclose some of your personal and sensitive information to our payroll, invoicing and data storage and records management services located overseas, including in the USA, United Kingdom, New Zealand, Singapore, Malaysia, Vietnam, and the Philippines. You agree to this disclosure and acknowledge that such recipients may use de-identified employee data for that recipient's commercial purposes. We will ensure that all arrangements with third party tools or platforms or third-party service providers will contain appropriate controls (which may be contractual or operational) to protect your personal information.

If you have any questions or would like to access your personal information held by auDA, please contact us at privacy@auda.org.au.

Occupational Health and Safety

In the context of OHS policies, procedures, training and instruction, as detailed in Section 25 of the *Occupational Health and Safety Act 2004* (Vic), employees are responsible for ensuring they:

- Follow reasonable instruction
- Cooperate with their employer
- At all times, take reasonable care for the safety of themselves and others in the workplace.

Flexible working arrangements

We believe in supporting our employees in balancing their work and life commitments. All roles at auDA can be worked flexibly by mutual agreement. This underpins a diverse, adaptive and high-performing workforce. The nature and scope of flexible options available will depend on the nature of the position. Applicants are encouraged to discuss flexible arrangements with the hiring manager during the recruitment process.

Please note that the role may require you to work the hours which are reasonably necessary to fulfil the requirements of the position, or as required by auDA, including monitoring, reading and responding to business-related communications from auDA or customers outside of usual office hours, where reasonable. The remuneration for this role includes compensation for all hours you would be required to work, including reasonable availability out of hours

Last Updated

25/08/2025