Position Description

Job title:	Security Analyst
Department:	IT
Work type:	Full Time
Reports To:	Information Security Officer
Position Reports:	Nil
Position Contact:	Adam King

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

Contribute: locally and globally

We serve all Australians and global internet users.

Better together

We collaborate and work together as one auDA.

Strive for excellence

We deliver value. On time, every time.

Role purpose

The Security Analyst plays a critical role in protecting the organisation's IT systems, infrastructure, and data from threats and vulnerabilities. As part of the Information Security team at auDA, the Security Analyst is responsible for monitoring, analysing, and responding to security incidents and risks while contributing to the continuous improvement of the organisation's security posture.
The role will assist with the management of the governance, risk and compliance frameworks within auDA and help to enforce the best security practices from various industry defined security standards including ISO 27001 and ISO 22301.

Key accountabilities

The primary responsibilities of the Security Analyst include:
Security Monitoring and Incident Response

- Analyse, triage, and respond to security alerts and events, prioritising events, including identifying root causes and recommending mitigation strategies.
- Conduct threat hunting and detection activities to proactively identify potential vulnerabilities and threats.
- Assist in developing and executing security incident response processes, ensuring timely resolution and documentation of incidents.

System Security, Physical Security and Patch Management

- Implement, configure, maintain, and operate tools to protect critical IT systems and data.
- Support the remediation of vulnerabilities identified through penetration tests, vulnerability scans, and other assessments.

Policy and Compliance Support

- Assist in reviewing and updating security policies, procedures, and incident response plans.
- Provide input to ensure compliance with relevant standards, such as ISO27001 ISO 22301 and Essential 8.
- Maintain accurate and updated knowledge base documentation related to security practices and configurations.

Collaboration and Knowledge Sharing

- Work with internal teams to ensure security requirements are integrated into projects and operations.
- Contribute to training and awareness programs for staff on security best practices and compliance requirements.
- Assist in the development and execution of disaster recovery and business continuity plans.

Other Responsibilities

- Incorporate Cyber Threat Intelligence practices, such as monitoring threat actor activity and identifying potential threats relevant to the ccTLD sector.
- Leverage scripting languages (e.g., Python, PowerShell) to automate repetitive security tasks and improve efficiency.
- Participate in testing and monitoring system performance to ensure alignment with security objectives.
- Validate backup and restore processes and verify data for key systems
- Assist with security control reviews
- Other activities as directed by the Information Security Officer and relevant executive leadership to support the organisation's strategic goals.

Key selection criteria

Technical Expertise

- Demonstrated understanding of security principles, techniques, and technologies (e.g., EDR, XDR, PKI, DLP, IDS, Zero Trust).
- Proficiency with operating systems (Windows, UNIX, and Linux) and tools such as Crowdstrike, Syslog, and SumoLogic.
- Knowledge of cloud computing environments and associated security frameworks (Microsoft Azure and AWS).
- Knowledge of Identity and Access Management principles

Analytical and Communication Skills

- Strong written and verbal communication skills, with the ability to produce high-quality documentation.
- Experience in translating technical security concepts for both technical and non-technical audiences.
- Proven ability to identify, analyse, resolve, and escalate issues effectively.

Compliance and Standards Knowledge

- Familiarity with ISO 27001, ISO 22301, Essential 8 and ITIL frameworks.
- Experience with risk management practices, including conducting risk assessments and gap analyses.

Teamwork and Adaptability

- Demonstrated ability to work effectively in a multidisciplinary team and independently.
- Strong organisational and multitasking skills, with the capacity to manage multiple priorities.
- Ability to handle stress and respond to challenges in high-pressure environments.

Additional Competencies Desired

- A solid understanding of DNS operations, DNSSEC, and threats unique to the ccTLD environment.
- Experience with tools like DNS monitoring and filtering solutions to detect and mitigate DNS-based attacks.

- Familiarity with user and entity behaviour analytics (UEBA) to identify anomalous behaviour that might indicate insider threats or compromised accounts.

Qualifications and experience

- Associate or bachelor's degree in Computer Science, Information Technology, System Administration, a closely related field or appropriate commercial experience.
- 1-3 years of proven experienced in a dedicated security role within large/complex environment
- 5 years experience in a System Administrator role (Windows or Linux)
- Experience or certification in ITIL Service Management framework.
- Experience or certification in Microsoft/Azure disciplines
- Experience of certification in AWS (foundation/professional/associate) an advantage

Other

Occasional work outside business hours will be required. Occasional domestic travel and potentially international travel may be required.

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 also be conducted. Where applicable, international background checks may also be required.

Privacy collection information

.au Domain Administration Limited ACN 079 009 34 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 use third party service providers including data storage and cloud services, some of which have servers located overseas, including the USA and you consent to this disclosure. We require that our service providers only use your information for authorised purposes and have appropriate controls 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

02 December 2024