POSITION DESCRIPTION

Cyber Security Engineer

ReadyTech (ASX:RDY) exists to help communities thrive, and ReadyTechers flourish on making that change happen.

They enjoy taking on challenges that matter to our customers, communities, and the world – and working to solve them with incredible technology that helps navigate complexity, while also delivering meaningful outcomes.

ReadyTechers are enterprising, and hungry to make a difference. But, more than ever, ReadyTechers are *ready for anything.*

POSITION DESCRIPTION

Title	Cyber Security Engineer	**Location**	Sydney, Melbourne, Launceston
Report to	Head of Platform Engineering	**Direct report(s)**	

The purpose of this role

This role exists to protect ReadyTech's critical technology platforms and services by designing, implementing, and maintaining robust cyber security controls. The position plays a key part in reducing risk, strengthening our security posture, and enabling the business to operate safely and with confidence.

The key accountabilities of the role

- Accountable for improving and maintaining the security posture of ReadyTech's AWS and Azure environments.
- Leading vulnerability management, threat detection, and remediation activities across our cloud platforms.
- Ensuring platform-level security aligns with frameworks such as Essential Eight, IRAP, ISO27001, SOCI and privacy standards.
- Driving the secure configuration of infrastructure as code, identity, network, and workload services in AWS and Azure.
- Acting as a key partner to the Platform Engineering team, embedding security practices into platform build and operations.

The key responsibilities of the role

- Design, implement and operate security controls in AWS and Azure, including IAM, network security, logging, and workload protection.
- Drive vulnerability scanning, threat monitoring, and configuration hardening in our cloud environments.
- Work closely with the Platform Engineering, Development & Security Operations teams to embed security into infrastructure and CI/CD pipelines.
- Optimise and maintain cloud-native and third-party security tools such as GuardDuty, Inspector, Security Hub, Microsoft Defender for Cloud, Sentinel, Wiz, Prowler and others.

- Conduct security reviews of platform changes and new cloud services to identify and mitigate risks.
- Develop and maintain security standards, patterns, and playbooks specific to AWS and Azure.
- Support incident response efforts related to cloud platforms and drive continuous improvements.

The ideal candidate will have these:

1. Skills	Ability to design, implement and maintain security controls in multi-cloud and on-premises environments. Strong scripting or automation capability (PowerShell, Python, Bash). Clear communication skills, able to translate technical concepts to diverse stakeholders.
2. Knowledge	Deep understanding of AWS and Azure security services, identity and access management, logging and monitoring, encryption, and secure networking. Working knowledge of frameworks such as Essential Eight, ISO27001, SOCI, and how they apply to cloud environments.
3. Experience	At least 5 years in cyber security or cloud engineering roles with a strong focus on securing AWS and Azure environments. Hands-on experience with Azure And AWS. Exposure to infrastructure as code and CI/CD security practices is highly regarded. Certifications such as AZ-500, SC-200, AWS Security Specialty, CISSP or OSCP highly regarded.