POSITION DESCRIPTION

Penetration Tester

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	Penetration Tester	**Location**	TBC
Report to	Head of Security Operations	**Direct report(s)**	

The purpose of this role

The purpose of the Penetration Tester role is to independently assess, challenge, and strengthen ReadyTech's security posture. This role conducts objective security testing across applications, infrastructure, and processes, operating separately from development and delivery teams to ensure unbiased evaluation. The Penetration Tester identifies security flaws, gaps, and risks, and works collaboratively with technology, governance, and operational teams to uplift security practices, improve resilience, perform code reviews, and support alignment with industry standards and compliance frameworks. Through proactive testing, guidance, and continuous improvement, the role contributes to building a secure, threat-resilient environment across the organisation.

The key accountabilities of the role

1. **Independent Security Testing**
   - Conduct penetration tests and security assessments across applications, cloud environments, and infrastructure, independently from development and delivery teams.
2. **Vulnerability Identification & Risk Assessment**
   - Identify, validate, and prioritise vulnerabilities and security gaps, providing clear risk insights aligned to business impact.
3. **Security Uplift & Collaboration**
   - Work with engineering, DevOps, and security teams to communicate findings and support effective remediation and security practice uplift.
4. **Continuous Security Improvement**
   - Recommend enhancements to security controls, processes, and testing methods to improve overall organisational resilience.
5. **Compliance & Standards Alignment**
   - Support alignment with IRAP, SOC 2, ISO 27001, and other relevant security and compliance frameworks.
6. **Threat Intelligence & Proactive Testing**
   - Stay current with emerging threats and apply this knowledge to proactively test ReadyTech systems.
7. **Reporting & Communication**
   - Produce clear, actionable reports and communicate findings to both technical and non-technical stakeholders including customer attestation evidence, audit documentation, and compliance reporting.
8. **Ethical and Responsible Conduct**
   - Perform all testing within approved scope, following ethical hacking standards and safeguarding sensitive data.

The key responsibilities of the role

- Conduct independent penetration testing across applications, networks, APIs, and cloud environments using methodologies consistent with industry-recognised certifications (e.g., CEH, OSCP, OSWE, GWAPT).
- Apply ethical hacking techniques, exploit development skills, and adversarial thinking that align with the capabilities validated through external penetration-testing qualifications.
- Perform advanced manual testing to identify complex vulnerabilities and business logic flaws, leveraging skills in reconnaissance, enumeration, exploitation, privilege escalation, and post-exploitation.
- Review system architecture, configurations, and—where required—source code, applying secure-coding and vulnerability-analysis knowledge aligned with CEH/OSCP/OSWE-level standards.
- Provide high-quality remediation guidance and technical uplift to engineering, DevOps, and security teams, informed by best practices from recognised security certification bodies.
- Maintain detailed testing documentation, methodologies, and evidence in a manner consistent with professional penetration-testing standards and compliance expectations (IRAP, SOC 2, ISO 27001).
- Contribute to developing and maturing ReadyTech's internal penetration-testing frameworks, adopting techniques and methodologies from leading certification programs and industry bodies (e.g., OWASP, SANS).
- Continuously update skillsets by tracking emerging vulnerabilities, exploit techniques, and threat actor behaviour's, maintaining competency equivalent to CEH/OSCP-level professionals.

The ideal candidate will have these:

1. Skills	- Conducting penetration tests using industry-aligned techniques and toolsets (e.g., Burp Suite, Nmap, Metasploit, OWASP ZAP). - Manual vulnerability discovery, exploit validation, and risk assessment. - Identifying and analysing security weaknesses across web applications, APIs, cloud platforms, and infrastructure. - Communicating technical findings clearly to both technical and non-technical audiences. - Writing structured, high-quality reports and documentation. - Problem-solving, critical thinking, and applying an adversarial mindset during testing. - Collaborating effectively with engineering, DevOps, and cybersecurity teams.
2. Knowledge	- Common vulnerabilities and exploitation techniques (e.g., OWASP Top 10, SANS Top 25). - Secure development practices and common coding flaws (e.g., injection, access control issues). - Network and application security fundamentals, including authentication, encryption, and cloud security concepts. - Ethical hacking frameworks and methodologies aligned with qualifications such as CEH, OSCP, OSWE, GWAPT, or similar. - Compliance frameworks relevant to the organisation such as IRAP, SOC 2, and ISO 27001, and how penetration testing supports these. - Threat landscapes, attacker behaviours, and modern exploitation tooling.

3. Experience	- Performing penetration tests or structured security assessments (professional experience or lab-based training acceptable for junior/mid-level). - Using recognised penetration-testing tools and scripting languages (e.g., Python, Bash, PowerShell) to aid testing activities. - Working with cloud environments (AWS/Azure/On Prem) and understanding common misconfigurations. - Applying hacking and secure-testing practice in line with certification standards. - Preparing penetration test reports and remediation guidance. - Participating in capture-the-flag events, home labs, or self-directed security research (For early-career/junior candidates).

4. Performance Indicators	- **Quality of Testing Activities**
	  ○ Thoroughness of penetration tests and accuracy of vulnerability identification.
	  ○ Adherence to approved testing methodologies and guidelines.
	- **Reporting & Communication**
	  ○ Clarity, accuracy, and usefulness of penetration test reports.
	  ○ Ability to communicate risk and remediation guidance effectively.
	- **Security Uplift Contribution**
	  ○ Demonstrated impact on reducing vulnerabilities and improving security controls.
	  ○ Quality of collaboration with development, DevOps, and product teams.
	- **Continuous Improvement**
	  ○ Adoption of new techniques, tools, and threat intelligence.
	  ○ Participation in uplift of internal testing methods, documentation, and processes.
	- **Compliance & Evidence Support**
	  ○ Timeliness and quality of evidence provided for IRAP, SOC 2, and ISO 27001 activities.
	  ○ Consistency of testing documentation with compliance expectations.

5. Qualifications	- CEH, OSCP, OSWE, GWAPT, or similar.