TALENT UNLIMITED

Helping Clients Succeed

www.thetalentunlimited.com
Mob: **+923213787471**
asad@thetalentunlimited.com

TALENT UNLIMITED is one of the rapidly growing HR consultancy firm providing exceptional management and consultancy services to organizations nationwide and beyond the boarder helping leaders navigate human capital challenges during times of growth and change. We bring deep and functional expertise in human resources to capture the value across boundaries and between the silos of any organization. The thrust and mission of our firm is to partner with organizations to improve performance through their most important resource that is their human resource.

SERVICES:

- ✧ HR Services
- ✧ IT Services & Resource Augmentation
- ✧ BPO Services
- ✧ Talent Incubation

LOOKING FOR CLOUD SECURITY ENGINEER FOR UAE

1. Organization Unit Purpose (why does the unit exist? What are the results the unit is expected to deliver?)

The unit's primary purpose is to Design, Engineer & eventually Embed practical & balanced cyber / information security principles/patterns/controls into all products and platforms. Conduct security assessments, gap analysis, provide remediation to the relevant squads / stakeholders.

2. Job Purpose (Why does the job exist? What is the unique contribution made by the job holder?)

Primary/General Job Purpose:

- Encourage 'Shift Left' Mindset - Proactively embed security requirements, by influencing implementation of security & privacy patterns from the start of the development cycle
- Implement via Influence - Influence stakeholders such as Product Owners, Solution Architects, Developers, Testers, Engineers & others to include security patterns into features, epics and stories in order to build secure, innovative & superior digital products for customers and employees
- Assessments – Perform security assessment and perform gap analysis to provide appropriate remediations to the teams for implementing the fixes.

  Key Skills – Application Security, Security Code review, API security, Platform security, IAST, SAST, DAST, Infrastructure security and Cloud Security – MS Azure

- **Tools and Technologies – Expertise in Azure Security Center and Azure Policies, Burp Suite, Nessus, Checkmarx, Kubernetes, Docker, Jenkins, GitHub, OpenShift and good knowledge about microservice architecture and pipeline driven security.**

Experience with following Components:

3. Technical Requirements

Application Security Assessment Skillset	1. Web Application Security 2. Security Code Review 3. Azure and AWS Cloud Security config review 4. Azure Virtual Desktop - AVD Security Review 5. Container Review 6. WAF rules review

Azure Security	Experience with following Components: 1. Azure Security Center 2. Azure AD RBAC 3. Privileged Identity Management 4. Conditional Access Policies 5. Azure Advanced Threat Protection 6. Azure Information Protection and HYOK 7. Enterprise mobility with Intune MAM and MDM Policies 8. Office365 ATP and Mail-flow 9. Microsoft cloud threat intelligence 10. Microsoft Cloud Application Security – CASB setup and monitoring 11. Windows Defender ATP 12. Policy configuration for Onedrive, Sharepoint, Outlook, Teams and Office Pro Plus 13. Azure AD Hybrid Join and Password Hash Sync 14. Customer Lockbox and advanced compliance policies in Azure cloud 15. AIP Data classification and reviewing DLP policies
Soft Skills:	• Ability to collaborate with multiple stakeholders and manage their expectations from a security perspective. • Holistic thinking; must balance security and functionality using practical demonstrable examples. Must also contribute to and implement "good architecture principles" to lower technical debt. • Assertive personality; should be able to hold her/his own in a project board or work group setting. • Superlative written and verbal communication skills; should be able to explain technical observations in an easy-to-understand manner. • Ability to work under pressure and meet tough/challenging deadlines. • Influencer- must be able to convince various stakeholders (internal IT Teams, C-Level execs, Risk & Audit) of why a certain observation is a concern or not
	• Strong understanding of Risk Management Framework and security controls implementation from an implementer standpoint • Has strong decision making, planning and time management skills. • Can work independently. • Has a positive and constructive attitude.

4. Person Specifications (required to carry out the job, not what the current or recommended incumbent possesses)		
Specifications	**Description of Knowledge / Skill etc.**	**Desirable or Essential**
A. Education • General • Professional	Bachelor's degree in a computer-related field such as computer science, cyber/information security discipline, physics, mathematics or similar	**Essential**
	• **General Information Security**: CISSP, OSCP, CEH, CISM/CISA or similar • **General Cloud Security**: CCSK /CCSP or similar • **Specific Cloud Security**: AWS/Azure/GCP/Oracle Solution/Security or similar • **Network Security**: CCNA, CCNP, CCIE, Certified Kubernetes Security Specialist	Desirable
B. Experiences (Years & Type) • Industry • Regional • Functional	Must have minimum 4 years of experience in an information security function with good background in information technology, stakeholder management and people management	**Essential**
	Minimum 3 years of experience, as a Security Engineer especially in Cloud Native environments	**Essential**
C. Knowledge & Skills • Technical • Functional • Managerial	Deep foundational knowledge, understanding and application on all aspects of Information Security concepts from broad range of technical and non- technical areas (Technical)	**Essential**
	Expert at the technology and frameworks in his/her area of expertise, and coach other architect on development standards and best practices.	Desirable
	Good understanding of enterprise level target architecture and public and private cloud platforms (IaaS/PaaS)	Desirable
	Good hands-on experience solutioning technology architectures that involve perimeter protection, core protection and end-point protection/detection & API /Micro services Security	Desirable
	Experience working in a DevOps environment with knowledge of Continuous Integration, Containers, DAST/SAST tools and building Evil Stories (Technical)	**Essential**

	Good knowledge of the concerns and threats that revolve around Cloud Security and how those concerns can be mitigated (Technical)	**Essential**
	The Analyst / Engineer has the skill to follow design principles and applies design patterns to enforce maintainable and reusable patterns, in the form of code or otherwise	Desirable
	The Analyst / Engineer can understand and interpret potential issues found in source or compiled code	Desirable
	The Analyst / Engineer has automation skills/capability in the form of scripting or similar	Desirable
	The Analyst / Engineer can attack application and infrastructure assets, interpret threats, and suggest mitigating measures	Desirable
	Ability to interpret Security Requirements mandated by oversight functions and ensure comprehensive coverage of those requirements, via documentation, within high level design and/or during agile ceremonies, via Evil Stories	Desirable
	The Analyst / Engineer can propose options for solutions to the security requirements / patterns that provide a balance of security, user experience & performance	Desirable
	The Analyst / Engineer has the skill to discuss and present solutions to other architecture, security, development, and leadership teams.	Desirable
	The Analyst / Engineer can interpret and understand vulnerability assessment reports and calculate inherent and/or residual risks based on the assessment of such reports	Desirable
	Ability to articulate and be a persuasive leader who can serve as an effective member of the senior management team. Good negotiation skills will be desirable	Desirable
	Must have good judgment skills to decide on an exception approval	Desirable
	Ability to enforce improvements when necessary, using Influence rather than Policing measures	Desirable
	Superior written and verbal communication skills to effectively communicate security threats and recommendations to technical or non-technical stakeholders	Desirable

	Knowledge of application of Agile methodologies/principles such as Scrum or Kanban	Desirable
D. Behavioral Competencies • Thinking Related • People Related • Self Related	- Influencer/Security Evangelist for the Team/Squad - Positive & Constructive Attitude - Autonomous worker / Decision Maker - Good listener - Patient & Calm during stressful situations - High energy individual / Motivator - Win-Win Attitude - Hacker/Defense-In-Depth mindset - Analytical thinking - Team Player/Interpersonal Skills - Eye for detail - Persistent & Persuasive - Organized / Structured - Deadline oriented - Competent and committed - People's Person; understands stakeholder management - Empathetic	All Essential
	- Passionate about architecting smart solutions - Innovator/Out of the box thinker - Collaborative Leadership style - Confident Presenter	
E. Personal Profile • Age • Nationality • Gender • Any Other	• Age – No bar • Nationality – No bar • Gender – No bar	

- End of the Document -