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 INFRASTRUCTURE SECURITY ENGINEERFOR UAE

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

The formation of the Group Information Security function is to ensure bank's information and data is resilient against external and internal security threats embed information security mindset as a core element of organization business strategy and provide an independent objective view of bank's security posture to the management committees The unit exists to provide secure banking environment for our customer and employees.

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

Primary/General Job Purpose:

- Assess the security and compliance of infrastructure and application technologies by them for weaknesses to protect customers and employees from attacks.
- Encourage 'Shift Left' Mindset - Proactively embed security requirements, by influencing implementation of security & privacy patterns from the start of the development cycle
- Assessments – Perform security assessment and perform gap analysis to provide appropriate remediations to the teams for implementing the fixes.
- **Responsible for security on infrastructure – OS, databases, virtual private networks, Software defined data centers, Proxies, Firewalls, Data Centre, Active Directory etc.**

  Key Skills – Infrastructure Security, IaaS and IaaC – Infrastructure as a Service and Infrastructure as a code, Platform security, Vulnerability and compliance assessment, application assessment, Security code review, Configuration reviews and Audits for network components and appliances, Active Directory Penetration testing.

  Tools and Technologies – Expertise in Ansible, Terraform, Kubernetes, Docker, Jenkins, Openshift and good knowledge about microservice architecture and pipeline driven security.

- Understanding of cloud computing technologies. Optionally, demonstrated hands on experience for performing security assessments for one or more of the following:
  1. **Core IaaS: Compute, Storage, Networking, High Availability**
  2. **Infrastructure: Security assessment on Switches, Firewalls, Routers.**
  3. **IaaC: Infrastructure as a Code – Security review expertise on IaaC platforms such as Ansible and Jenkins.**
  4. **Security Code review**
  5. **Azure PaaS Services: Redis Cache, Service Bus, Event Hub, Cloud Service, IoT suite, Mobile Apps, etc. Preferrable: Cosmos DB, Azure Kubernetes Service**
  6. **Experience in one or more automation languages (like Python)**

3. Technical Requirements

Application Security Assessment Skillset	1. Infrastructure review – Security reviews for network appliances and data centres. 2. Configuration reviews for switches, routers Firewalls. 3. Active Directory Penetration Testing 4. Infrastructure as a Code review. 5. Review of VMs and hypervisors. 6. Vulnerability Assessment and Penetration testing 7. Security Code review - Ansible / Jenkins script review 8. Container Security 9. Docker Review / Image review 10. Open-source Libraries review 11. Application Security 12. WAF rules review 13. Policy review for firewalls, proxies etc

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**
Education • General • Professional	Bachelor’s degree in a computer-related field such as computer science, cyber/information security discipline, physics, mathematics or similar	Desirable
	Master’s degree in business administration, information security, human resource management, finance or international business or executive education from reputed institutes like Harvard	Desirable
	• Security Pentest: OSCP, GPEN, LPT, CPT or similar • General Information Security: CISSP, CISM/CISA or similar • Network Security: CCNA, CCNP, CCIE, Certified Kubernetes Security Specialist • General Cloud Security: CCSK /CCSP or similar • Specific Cloud Security: AWS/Azure/GCP/Oracle Solution/Security or similar	Desirable
B. Experiences (Years & Type) • Industry • Regional • Functional	Must have a minimum 4-9 years of experience in an information security function with good background in information technology, stakeholder management and people management	Essential
	Minimum 3-5 years’ experience, as a Security Engineer especially in Cloud Native environments	Desirable
	Minimum 3-5 years’ experience as a Network Security Engineer	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) Good understanding of enterprise level target architecture and public and private cloud platforms (IaaS/PaaS) Good hands on experience solutioning technology architectures that involve perimeter protection, core protection and end-point protection/detection Experience working in a DevOps environment with knowledge of Continuous Integration, Containers, DAST/SAST tools and building Evil Stories (Technical) Good knowledge of the concerns and threats that revolve around Cloud Security and how those concerns can be mitigated (Technical)	Essential Essential Essential Essential
	The Analyst / Engineer has the skill to follow design principles and applies design patterns to enforce maintainable, readable and reusable patterns, in the form of code or otherwise The Analyst / Engineer can understand and interpret potential issues found in source or compiled code The Analyst / Engineer has automation skills/capability in the form of scripting or similar The Analyst / Engineer has the ability to attack application and infrastructure assets, interpret threats and suggest mitigating measures 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 The Analyst / Engineer can propose options for solutions to the security requirements / patterns that provide a balance of security, user experience & performance The Analyst / Engineer can interpret and understand vulnerability assessment reports and calculate inherent and/or residual risks based on the assessment of such reports Must have good judgment skills in order to decide on an exception approval Superior written and verbal communication skills in order to effectively communicate security threats and recommendations to technical or non-technical stakeholders Knowledge of application of Agile methodologies/principles such as Scrum or Kanba	Essential Essential Essential Essential Essential Essential Essential Essential Essential

D. **Behavioral Competencies** • Thinking Related • People Related • Self Related	- Influencer/Security Evangelist for the Team/Squad - Positive & Constructive Attitude - Autonomous worker / Decision Maker - Patient & Calm during stressful situations - High energy individual / Motivator - 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	All Desirable
E. **Personal Profile** • Age • Nationality • Gender • Any Other	• Age – No bar • Nationality – No bar • Gender – No bar	

- End of the Document -