



# TALENT UNLIMITED

Helping Clients Succeed

[www.thetalentunlimited.com](http://www.thetalentunlimited.com)

Mob: +923213787471

[asad@thetalentunlimited.com](mailto: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 DEVOPS SECURITY ENGINEER FOR UAE

<b>1. Organization Unit Purpose</b> (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.	
<b>2. Job Purpose</b> (Why does the job exist? What is the unique contribution made by the job holder?)	
<p>Primary/General Job Purpose:</p> <ul style="list-style-type: none"> <li>• Encourage 'Shift Left' Mindset - Proactively embed security requirements, by influencing implementation of security &amp; privacy patterns from the start of the development cycle</li> <li>• Implement via Influence - Influence stakeholders such as Product Owners, Solution Architects, Developers, Testers, Engineers &amp; others to include security patterns into features, epics and stories in order to build secure, innovative &amp; superior digital products for customers and employees</li> <li>• Assessments – Act as a DecSecOps engineer to Perform security assessment, gap analysis to provide appropriate remediations to the teams for implementing the fixes.</li> </ul> <p><b>Key Skills –Container Security, Machine Learning and Analytics Security Review, Security Code review, API security, Platform security for open-source technologies for Platform as a Service technologies, Python / R knowledge</b></p>	
<b>3. Technical Requirements</b>	
Security Assessment Skillset	<ol style="list-style-type: none"> <li>1. Machine Learning security assessment skillsets – Code review for Python based code and sound knowledge on Machine learning and AI using python.</li> <li>2. b. Good understanding of Keras, Tensorflow and other AI related frameworks.</li> <li>3. c. Excellent knowledge of embedding security into CI/CD pipelines using Jenkins, Argo CD</li> <li>4. d. Excellent with docker / K8s based containers</li> <li>5. e. Should have minimum experience of 2 years in managing security for Onpremise Kubernetes cluster. Knowledge on Cloud K8S clusters would be an added advantage.</li> <li>6. Good with Security assessment for big data platform – Cloudera platform</li> <li>7. Should have hands-on experience in security review of queue management systems such as Kafka.</li> <li>8. Mandatory certifications required – CKA (Certified Kubernetes Administrator) and CKS (Certified Kubernetes Security Specialist)</li> </ol>
Skills:	<ul style="list-style-type: none"> <li>• Ability to collaborate with multiple stakeholders and manage their expectations from a security perspective</li> <li>• Holistic thinking; must balance security and functionality using practical demonstrable examples. Must also contribute to and implement "good architecture principles" to lower technical debt</li> <li>• Assertive personality; should be able to hold her/his own in a project board or work group setting</li> <li>• Superlative written and verbal communication skills; should be able to explain technical observations in an easy-to-understand manner</li> <li>• Ability to work under pressure and meet tough/challenging deadlines</li> <li>• Influencer- must be able to convince various stakeholders (internal IT Teams, C-Level execs, Risk &amp; Audit) of why a certain observation is a concern or not</li> <li>• Strong understanding of Risk Management Framework and security controls implementation from an implementer standpoint</li> <li>• Has strong decision making, planning and time management skills.</li> <li>• Can work independently.</li> <li>• Has a positive and constructive attitude.</li> </ul>

**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
<p><b>A.</b></p> <p><b>Education</b></p> <ul style="list-style-type: none"> <li>• General</li> <li>• Professional</li> </ul>	<p>Bachelor’s degree in a computer-related field such as computer science, cyber/information security discipline, physics, mathematics or similar</p> <ul style="list-style-type: none"> <li>• <b>General Information Security:</b> CISSP, OSCP, CEH, CISM/CISA or similar</li> <li>• <b>General Cloud Security:</b> CCSK /CCSP or similar</li> <li>• <b>Kubernetes Security:</b> CKA / CKS</li> <li>• <b>Specific Cloud Security:</b> AWS/Azure/GCP/Oracle Solution/Security or similar</li> <li>• <b>Network Security:</b> CCNA, CCNP, CCIE,</li> </ul>	<p><b>Essential</b></p> <p>Desirable</p> <p><b>Essential</b></p> <p>Desirable</p>
<p><b>B.</b></p> <p><b>Experiences (Years &amp; Type)</b></p> <ul style="list-style-type: none"> <li>• Industry</li> <li>• Regional</li> <li>• Functional</li> </ul>	<p>Must have minimum 4 years of experience in an information security function with good background in information technology, stakeholder management and people management</p> <p>Minimum 3 years of experience, as a Security Engineer especially in Cloud Native environments</p>	<p><b>Essential</b></p> <p><b>Essential</b></p>

<p><b>Knowledge &amp; Skills</b></p> <ul style="list-style-type: none"> <li>• Technical</li> <li>• Functional</li> <li>• Managerial</li> </ul>	<p>Deep foundational knowledge of Containerized environment and CI/CD pipeline</p>	<p><b>Essential</b></p>
	<p>Expert at the technology and frameworks in his/her area of expertise, and coach other architect on development standards and best practices.</p>	<p>Desirable</p>
	<p>Good understanding of Microservice based architecture (Technical)</p>	<p>Desirable</p>
	<p>Good hands-on experience solutioning technology architectures that involve perimeter protection, core protection and end-point protection/detection &amp; API /Micro services Security</p>	<p>Desirable</p>
	<p>Experience working in a DevOps environment with knowledge of Continuous Integration, Containers, DAST/SAST tools and building Evil Stories (Technical)</p>	<p><b>Essential</b></p>
	<p>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</p>	<p>Desirable</p>
	<p>The Analyst / Engineer can understand and interpret potential issues found in source or compiled code</p>	<p>Desirable</p>
	<p>The Analyst / Engineer has automation skills/capability in the form of scripting or similar</p>	<p>Desirable</p>
	<p>The Analyst / Engineer can attack application and infrastructure assets, interpret threats, and suggest mitigating measures</p>	<p>Desirable</p>
	<p>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</p>	<p>Desirable</p>
<p>The Analyst / Engineer can propose options for solutions to the security requirements / patterns that provide a balance of security, user experience &amp; performance</p>	<p>Desirable</p>	

	<p>The Analyst / Engineer has the skill to discuss and present solutions to other architecture, security, development, and leadership teams.</p> <p>The Analyst / Engineer can interpret and understand vulnerability assessment reports and calculate inherent and/or residual risks based on the assessment of such reports</p> <p>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</p> <p>Must have good judgment skills to decide on an exception approval</p> <p>Ability to enforce improvements when necessary, using Influence rather than Policing measures</p> <p>Superior written and verbal communication skills to effectively communicate security threats and recommendations to technical or non-technical stakeholders</p> <p>Knowledge of application of Agile methodologies/principles such as Scrum or Kanban</p>	<p>Desirable</p> <p>Desirable</p> <p>Desirable</p> <p>Desirable</p> <p>Desirable</p> <p>Desirable</p> <p>Desirable</p>
<p><b>Behavioral Competencies</b></p> <ul style="list-style-type: none"> <li>• Thinking Related</li> <li>• People Related</li> <li>• Self Related</li> </ul>	<ul style="list-style-type: none"> <li>- Influencer/Security Evangelist for the Team/Squad</li> <li>- Positive &amp; Constructive Attitude</li> <li>- Autonomous worker / Decision Maker</li> <li>- Good listener</li> <li>- Patient &amp; Calm during stressful situations</li> <li>- High energy individual / Motivator</li> <li>- Win-Win Attitude</li> <li>- Hacker/Defense-In-Depth mindset</li> <li>- Analytical thinking</li> <li>- Team Player/Interpersonal Skills</li> <li>- Eye for detail</li> <li>- Persistent &amp; Persuasive</li> <li>- Organized / Structured</li> <li>- Deadline oriented</li> <li>- Competent and committed</li> <li>- People's Person; understands stakeholder management</li> <li>- Empathetic</li> <li>- Passionate about architecting smart solutions</li> <li>- Innovator/Out of the box thinker</li> <li>- Collaborative Leadership style</li> <li>- Confident Presenter</li> </ul>	<p>All Essential</p>

<b>Personal Profile</b> <ul style="list-style-type: none"><li>• Age</li><li>• Nationality</li><li>• Gender</li><li>• Any Other</li></ul>	<ul style="list-style-type: none"><li>• Age – No bar</li><li>• Nationality – No bar</li><li>• Gender – No bar</li></ul>	
--	---	--

- [End of the Document](#) -