Interested applicants please email resumes to Gabrielle Loh gabrielle.loh@leap.asia

Senior Security Consultant

Job Description

Department:	LEAP, a Company of ST Telemedia
Job Title:	Senior Security Consultant
Date:	21st May 2019

The Ideal Candidate

You are a highly motivated, bright, dynamic and adaptable business leader and individual contributor who thrives in an innovative, performance-oriented environment. Continual learning is everything and you want to be a key contributor in a team full of diverse, experienced technology and business professionals. Deep down you have a passion for life, embrace change and thrive in a creative environment. You understand what motivates customers and team members alike and you find solutions to their problems that are economic, strategic and elegant. How would others that you have worked with describe you? Is this you?

Joining the LEAP team gives you the opportunity to: work on a disruptive product that's still in its very early stages, solving challenging problems that will revolutionize enterprise computing in the cloud. You'll work for a hyper-growth company that is focused on creating the highest quality product in the market where your work has direct impact on customers every day.

Your Purpose:

We at LEAP strive to bring together a collection of cloud-based software products into an integrated offering with a unified experience. LEAP's delivery organization plays a pivotal role in ensuring that the best value that it's AI-led, cloud-based products and services are delivered in effectively and efficiently to every customer.

As the Senior Specialists you will own and manage the implementation of security solutions for our customers. LEAP delivers measurable business results through the rapid and effective adoption of new technology, including AI and cloud, and your role will include all of this in its scope. Business outcomes delivery is defined as a measured improvement in one or more business metrics, so you will implement the measurement system for this and use it as a key success measure of Business Value Realization. Adoption of new technology typically involves business process analysis and business process change and you will work with colleagues and the customer teams to implement these. Equally important is the successful deployment and integration of the new technology solutions and their integration into the customer's existing technology environment. You will have overall accountability for each customer delivery including all these areas

This role will provide ample opportunities for growth and you must possess drive and ambition to extend your skills into new areas of customer focus that will evolve as part of your role and the growth of the business. You must ensure the company's ability to deliver the proposed solutions and be able to demonstrate that your work delights our customers by delivering best-in-class Net Promoter Score (NPS) results.

The role is critical to the success of LEAP and will initially be an individual contributor role but has the potential to grow (based on success) to a lead a larger multi-disciplinary team as we scale out. The role is primarily customer-delivery-focused, but it is expected that you will work within the STT ecosystem to assist in the evaluation and execution of the overall business strategy including M&A, deal structuring, technology and business architecture.

Key Responsibilities (approximately 6-10):

Strategy & Planning

- Help customers analyze their overall security needs and determine technology roadmaps to address such needs.
- Security architecture- Design, Plan, Implement and Gap Analysis
- Lead creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures).
- Enterprise Business Continuity Plan and Disaster Recovery Plan- Plan & Design.

Key Responsibilities (continued):

Customer Acquisition & Deployment

- Maintain up-to-date, detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes, and the development of new attacks and threat vectors.
- Recommend appropriate security solutions and/or enhancements to existing security solutions to improve overall enterprise security.
- Onboard new customers, and play a hands-on role in implementing Security Solutions in customer environments
- Perform the deployment, integration, and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically, and the enterprise's security documents specifically.
- Evaluate new and possible cloud vendors on security features and advise the Strategic Sourcing Specialist on those that meet organizational security standards and policies.

Operational Management

- Maintain up-to-date baselines for the secure configuration and operations of all cloud, in-place devices, whether they be under direct control (e.g. security tools) or not (e.g. workstations, servers, network devices, etc.).
- Maintain operational configurations of all in-place security solutions as per the established baselines.
- Monitor all in-place security solutions for efficient and appropriate operations.
- Review logs and reports of all in-place devices, whether they be under direct control (e.g. security tools) or not (e.g. workstations, servers, network devices, etc.). Interpret the implications of that activity and devise plans for appropriate resolution.
- Drive investigations into problematic activity.
- Design and execution of vulnerability assessments, penetration tests, and security audits.
- Provide on-call support for end users for all in-place security solutions.
- Evaluate procured cloud services to ensure they are meeting existing security standards.
- Experience with integrating cloud-native API-based services into enterprise systems such as ticketing, workflow automation, and others

Knowledge & Experience

- Extensive experience with Security Devices included physical and virtual appliances, cloud based solutions. Experience with Cisco, Checkpoint, Paulo Alto etc.
- Working technical knowledge of Cloud Security Solutions, cloud (AWS, AZURE, GCP) security architecture & solutions.
- Strong understanding of LAN / WAN, IP, TCP/IP, and other network administration protocols.
- Practical expertise in various scripting and programming languages relevant to cloud development and integrations
- Strong understanding of Windows and Linux Operating Systems & Virtualization.
- Knowledge in developing and analysing conceptual and technical cloud reference architectures
- Knowledge in Cyber-Attack Simulation Testing, Pen Tests, Vulnerability Assessment are preferred.
- Experience adopting and implementing cloud security controls frameworks such as the CSA CCM, and various other cloud-specific derivatives
- Certifications such as CISA, CISSP, Cloud (AWS, Azure, GCP), various other cloud-security related technical Certifications will be an added advantage

Formal Education:

- College diploma or university degree in the field of computer science and/or two years equivalent work experience.
- One or more of the following certifications:
    - CompTIA Security+
    - GIAC Information Security Fundamentals
    - Microsoft Certified Systems Administrator: Security
    - CISA, CISSP, Associate of (ISC)2