Role: Penetration Testing/Red Team/AppSec Lead
Title: Senior Security Consultant/Engineer

Location – *Connecticut (Westport-HQ), New York, Boston, Atlanta. Miami,*
Philadelphia, Dallas, Chicago, Los Angeles, San Francisco, Washington DC - (All are
possible locations)

Lodestone Security, is seeking a senior consultant to continue the growth and
development of the firm's Security Posture Assessment Practice. As a Senior Security
Consultant you should have a blend of both internal practice development and external
client delivery capabilities as Lodestone capitalizes on its unique market position, as a
subsidiary of Beazley Insurance.

An ideal candidate finds themselves pulling things apart logically and physically to
discover their function and failings. They are not afraid to jump into the unknown, or lead
others down esoteric paths of knowledge. Lodestone prides itself with being on the
forefront of the industry, and needs talented individuals looking to contribute to both their
team and the industry as a whole. Research, tools development and automation are all
under the umbrella of this position, and expected in the ideal candidate. Do you enjoy
scanning networks, injecting payloads, reversing protocols, and fuzzing binaries;
Breaking things in the latest and greatest way? This might be a role for you.

The role requires a self-starter who can operate independently through the entire client
engagement process, from introduction calls to scoping, intel gathering and recon, to
reporting and proofreading. At the end of the day, Lodestone is still very much a start-up.
The right individual for the job is going to be ready to roll up their sleeves and do
whatever it takes to get the company off the ground. Tenacity and attitude are going to be
requirements here, not just nice to haves.

In addition, the candidate will be encouraged to create an external brand for the business,
through activities that could include – conference presentations, industry involvement
with both commercial entities and law enforcement, the production of in articles and
whitepapers, open source tools and other external activities, that will help create and
reinforce the Lodestone brand and market presence.

Although this role focuses on Posture Assessments, you will work hand in hand with our,
Incident Response and Strategic Assessment consultants to provide practical and holistic
security guidance for our clients. In addition to client-focused deliverables, you will have
responsibilities for developing repeatable methodologies based on industry standards as
well as tools for internal practice development.

About Lodestone:

Lodestone Security LLC was founded to address the unmet cyber security needs in the Small and Medium Business (SMB) market. In recent years, the SMB market has been victimized by a multitude of cyber security breaches. Lodestone is comprised of security professionals who have worked in the world's top professional services firms and Fortune 500, allowing Lodestone to offer a high level of expertise to its clients.

Core Requirements:
Essential Duties and Responsibilities may include:
- Ability to successfully interface with clients (internal and external)
- Ability to document and explain technical details in a concise, understandable manner
- Leading Attack and Penetration, Vulnerability assessment engagements against client networks, devices and applications.
- Writing clear and concise reports with actionable remediation and practical recommendations for both a business and technical audience. While adequately explaining, presenting and/or demonstrating [when applicable] the operational impact of a particular vulnerability/exploit.
- Developing curriculum and conducting training courses in network and application security; (including tabletop exercises)
- Conducting or leading research to bolster Lodestone's ability and reputation
- Building of tools, scripts, and infrastructure for the team, and/or open-sourced
- Managing projects and staff, and developing/mentoring less experienced staff
- Ability to work independently in a remote capacity

The ideal candidate will come from a professional consulting background, have experience as a senior penetration tester, application or network security engineer, or similar background. This individual must love pulling systems apart, physical or logical, to decipher their function and failings. The candidate must also have a desire to deliver excellent client service and have a passion for the profession and will feel comfortable working with both technical and business audiences, in the delivery of technical security assessment services.

The role is an ideal match for the following profiles:

1) An inquisitive individual who enjoys "breaking" systems, software, hardware and network environments, exposing security weaknesses, and developing ways to mitigate them.
2) A talented experienced Associate or Senior Consultant from a Leading Security Service Provider or Consultancy who is looking for an opportunity to apply their experiences in a startup environment and is motivated by delivery and client satisfaction.

Additional Enhancements:
- Previous experience or willingness to represent Lodestone Security in public forums including Conferences, Trade Associations, and other Community Related Activities.
- An entrepreneurial mind-set and willingness and desire to help build a service focused business.
- A desire for their compensation to be correlated directly with their success in the role.
- Knowledge or experience of DFIR and/or Risk Advisory practices and service.

Desired Skills
- Strong technical background across networking, operating systems, applications, databases, embedded systems, wireless, or respective area of penetration testing focus
- Expertise performing penetration testing, threat modeling, and security assessments
- Strong knowledge of tools and techniques used for penetration testing in respective area of penetration testing focus; network, application, wireless, IoT
- Capable of developing scripts and tools to automate common tasks
- Ability to provide training, perform public speaking and be comfortable and confident in front of an audience
- Experience architecting and developing applications, on a team or at scale
- Strong knowledge of tools and techniques used for reverse engineering applications, malware, hardware, etc.

Domain Knowledge:

Strength in at least two of the six domains:

- Embedded (IoT) analysis and/or development
- Wireless protocol analysis, Software Defined Radio attack and defense
- Social Engineering or assessing the physical security of organizations
- Application Security Reviews and exploitation; including static analysis/code review, dynamic testing on all execution stacks, including web, mobile, native etc.
- Network Security Assessment, analysis, and Exploitation
- Cryptanalysis, Machine Learning, or similar Data Science or Math background, experience or study

Education & Other Requirements

- A minimum of three years of experience working in the Information Security industry with a detailed focus on either Network Attack & Penetration, Application, Embedded, or Wireless Security.
- Must be eligible to work indefinitely in the U.S.
- Bachelor's or Master's Degree with a technical focus or in a related discipline or comparable work experience
- OSCP, GPEN, GWAPT, OSWE, CEH certifications a plus

The candidate will not be responsible for "direct sales" – but will be responsible for serving as the technical lead in following up on business opportunities derived from their relationship with Beazley and other channels. The selected candidate will also be expected to support in the recruitment of additional team members corresponding with the growth of the business. In addition they will have a leadership role in developing members of the consulting team.