**Depth Security – Security Consultant/Penetration Tester – Kansas City**

**Summary**
The primary role of a Senior Security Consultant at Depth Security is to perform multidisciplinary assessment services as needed. Examples include Application Security Assessments against web apps, mobile apps, web services, and fat-client applications. Proficiency in delivering Network Vulnerability and Penetration Assessments both externally and internally against wired and wireless targets is also required. Senior Security Consultants can assess external, internal, wired, and wireless networks. Social engineering assessments, both phishing-based and physical, may also be required occasionally. Senior Security Consultants must demonstrate the highest skill levels and help set acceptable assessment standards for the Company.

**Duties**
- Deliver Application Security Assessments against web apps, mobile apps, web services, and fat-clients
- Deliver External, Internal, and Wireless Vulnerability and Penetration Assessments
- Deliver highly targeted and specialized Red Team engagements
- Deliver phishing-based and physical Social Engineering Assessments
- Communicate with customers in a friendly manner, quickly and clearly, and with great accuracy during:
  - Kickoff and scoping calls
  - Assessment status updates and ongoing project communication
  - Report delivery
  - Wrap-up meetings
- Assist in enhancing various company methodologies
- Mentor Security Consultants and assist in their efforts to develop areas of expertise
- Demonstrate the highest level of offensive skills, pre and post-exploitation
- Demonstrate excellent writing skills both during email correspondence and report creation
- Prioritize findings based on perceived risk, using existing knowledge of clients’ business to ascertain finding severity
- Lead by example in behavior, work ethic, and punctuality
- Interpret and obey any applicable customer testing restrictions based on scope and kickoff calls
- Utilize non-billable time to work on company-directed internal projects
- Contribute to company methodology and vulnerability repositories
- Contribute to company blog and to company image via speaking engagements

**Requirements**
- Assessment experience with networks and applications
- Posses longer-term, multi-disciplinary, expert-level IT skills including sysadmin, infrastructure, net-engineering, software development, and security-engineer experience
- Applicants with common industry certifications such as OSCP, OSCE, SANS, CREST, and etc. will be preferred.
• Demonstrates knowledge of all classes of vulnerabilities and exploits
• Posses more blue-team knowledge than junior peers
• Should have numerous public vulns/exploits to name
• Identifies vulnerabilities and discloses on public software on an ongoing basis
• Writes exploits from scratch if necessary
• BurpSuite Expert
  o Ability to write BurpSuite Extender plugins
  o Ability to configure working login macros
  o Use Repeater and Intruder to manually find flaws.
  o Use Scanner in an appropriate manner to automatically find flaws.
  o Quickly eliminate false positive based on intuition and response content
• Burp Extender contributor
• Github
• Kali Ninja
• Metasploit Expert
• Scripting skills: Whatever gets the job done (php/perl/python/bash/etc)