Senior Cybersecurity Professional – Penetration Test/Red Team: Charleston SC

Position Overview

Security Risk Solutions, Inc., a professional information security services company in Charleston, SC, is seeking a Senior Cybersecurity Professional with extensive Penetration Testing/Red Team experience. Problem-solving and lateral thinking skills along with excellent written and verbal communication skills are essential.

In-depth knowledge of Federal and/or Department of Defense information Security and information security policies is required, along with the ability to conduct technical penetration tests and perform other sanctioned offensive cyber activities. This position requires a deep understanding of offensive cybersecurity techniques, attack vectors, threat profiles and the anatomy of cyberattacks.

This is a hybrid remote/in-person position, with approximately 75% remote/25% in person. Remote work includes leading and conducting penetration testing engagements for various information systems, developing reports, attending virtual meetings, and implementing post-testing process improvement activities. On-site work includes facilitating and participating in testing exercises with offensive cybersecurity testing teams and delivering presentations to system owners, technical teams, and executives.

This position requires direct interaction with customers and the ability to work with minimal supervision. The individual must represent the company in the best possible light and maintain the highest standards of professionalism. Flexibility, a willingness to learn, and a creative approach to problem solving are key.

US Citizenship and the ability to obtain and maintain a DoD security clearance are required.

Qualification and Experience Requirements:

- Bachelor's degree in Computer Science, Information Security, or related field required.
- Minimum 8 years direct Cybersecurity experience required.
- Must hold current CISSP certification, plus one or more of the following:
    - Offensive Security Certified Professional (OSCP)
    - Certified Ethical Hacker (CEH)
- Experience with security testing tools including: Kali Linux, Nmap, Burp Suite, SQLmap, and Metasploit
- Experience conducting offensive cybersecurity tests for various systems and technologies, including conducting remote, local privilege escalation, and client-side attacks
- Experience identifying and exploiting vulnerabilities associated with implementation of APIs
- Experience working in cyber lab environments and prior participation in war-game scenarios
- In-depth knowledge of Federal and/or Department of Defense cybersecurity policies, including NIST SP 800-53, SP 800-171, SP 8000-63, DISA STIGs, and the MITRE attack framework

Salary: Competitive salary, commensurate with experience.

Application Procedures: Cover letter with resume should be submitted to: jobs@securityrs.com

Additional Information:

- **Benefits:** Benefits include employee health insurance, retirement plan, flexible paid-time-off policy (15 days) plus 11 paid Federal Holidays. Visit www.securityrisksolutions.com for more information about the company.
- **E-Verify:** If you are selected for this position, the documentation that you present for purposes of completing the Department of Homeland Security (DHS) Form I-9 will be verified through the DHS "E-Verify" system. Federal law requires DHHS to use the E-Verify system to verify the employment eligibility of all new hires and obligates the new hire to take affirmative steps to resolve any discrepancies identified by the system as a condition of continued employment. Security Risk Solutions, Inc., is an E-Verify Participant.
- **Security Clearance:** US Citizenship and ability to obtain and maintain a DoD security clearance is required.