Role : Project Development Analyst - Application Security
Location : Houston, TX (the Woodlands)
Duration : 1 year

Candidate should have all of the following technical and professional characteristics as well:

- Min 6 years of experience penetration/vulnerability testing for web and thick-client applications in an enterprise environment
- Strong understanding of web technologies, e.g. HTTP, HTML, CSS, Forms, Database Connectivity, etc.
- Understanding of compliance and regulatory requirements such as PCI DSS, SOX, HIPAA, etc.
- Full grasp and ability to articulate and/or train others on the "OWASP Top 10" and related concepts
- Minimum 6 years of experience with programming and/or scripting in one or more of the following languages: .NET, Java, PHP, Ruby, Perl, Bash, or similar language
- Minimum 6 years of experience with SQL, including a strong understanding of SQL syntax and the ability to perform basic management of MS SQL databases
- **Ability to perform manual web application vulnerability assessments without the use of automated tools such as web application scanners**
- Ability to capture and analyse network traffic at all seven layers of the OSI model, including ability to discern whether said network traffic contains vulnerabilities and/or sensitive data
- Have a solid grasp of core security fundamentals and concepts, including knowing one's system, defence in depth, the principle of least privilege, access control, encryption and cryptography, security architecture and design, business continuity and disaster recovery, etc.
- Minimum 6 years of experience with enterprise-level security control implementations, including Network Intrusion Detection/Prevention (NIDS/NIPS), Corporate Antivirus, Enterprise Web Filtering, Data Loss Prevention, Insider-threat Mitigation, Botnet Detection, etc., as well as demonstrable knowledge of the principles and techniques used to bypass said controls.
- Ability to create extremely high quality written reports containing the findings from web and thick-client vulnerability assessments, as well as the ability to articulate those findings to peer technical staff as well as various levels of management
- Preference is for candidates with two or more of the following certifications: GSEC, GWAPT, CISSP, GPEN, GXPEN, CISA, CISM, OSCP, OSCE