Job description

Our value is in our employees – smart, passionate, perceptive and fun people.

Learn and Grow with us! Our innovations and employees impact the growth, success, and direction of our client's mission and our company. We all share a true passion for technology and enjoy working together to protect information systems, develop solutions, share ideas, and exchange knowledge. We celebrate diversity and the unique perspective each team member brings to his/her job, team, and community. We are currently seeking talented and motivated **Security Applications Engineers** for full or part-time positions.

Essential Functions:

- Support projects within the SDLC and Agile environments with applications security testing penetration testing and vulnerability management functions
- Perform Web / Mobile application security assessments and penetration testing on projects and/or releases; produce detailed risk reports with identified vulnerabilities and remediation recommendations
- Conduct static and dynamic code analysis as needed to support release cycles.
- Work closely with development team during the envisioning and development process to guide secure design and secure coding practices
- Manage web application firewall through log analysis, system tuning and rule development
- Evaluate, track, and ensure compliance of high and critical vulnerabilities; develop, maintain and update scorecards to reflect vulnerabilities and communicate to end users
- Implement security solutions, and provide technical leadership during the design, development, and testing phases of major initiatives
- Conduct security architecture reviews on existing technology and offer plans for remediation
- Scanning customer source code, auditing results with development and/or security teams and offering plans for remediation of vulnerabilities
- Work with enterprise architects and developers to design optimal security practices when developing new application functionality
- Mitigate security risks associated with projects, which have a high technical complexity and/or involve significant challenges to the business
- Advanced to expert level knowledge and understanding of architecture, application design, systems engineering and integration required
- Interpret business requirements and functional specifications to recommend security requirements

- Communicate technical application security concepts to customer staff, including developers, architects, and managers
- Work with development and QA teams to ensure the use of secure coding practices and verification methods
- Act as a Subject Matter Expert in the discovery and investigation of critical security vulnerabilities as required
- Conduct manual application security testing and source code auditing for a variety of technologies and code-types
- Collaborating with Product Management and Engineering to enhance products
- Ensure new system builds entail appropriate security packages, tools, logging and monitoring applications are configured properly
- Provide detailed risk and remediation guidelines, as well as perform remediation activities where applicable
- Collaborate with Development and Software Engineering teams to identify deficiencies in, improving company policies & procedures for, and executing on a Secure SDLC
- Lead in the development and providing guidance during architecture and design activities of new and existing applications, while also conducting architectural risk and impact assessments on new and existing applications
- Research and evaluate proposed software architecture solutions for adherence to documented company standards, policies, and regulatory responsibilities and work collaboratively with multidisciplinary teams and Business Units to implement and support existing and future solutions
- Maintain knowledge of current and emerging secure application technologies/products/trends related to architectural solutions; actively and continuously share this knowledge with others
- Communicate Findings/Remediation Guidance/Security Design Patterns to development teams in a concise and succinct manner
- Learn, create and support internal Security Design Review processes, Threat Modeling tools and infrastructure

Knowledge, Skills, Qualifications and Experience:

Required:

- Experience in secure development of largescale, user-facing web applications
- Experience in evaluating tools, technologies, and processes for best organizational fit

- Experience working with, and theoretical knowledge of front-end architectural topics (HTTP, Cookies, caching, web performance, scalability, security, third-party integrations)
- Hands-on experience with the following technologies:
    - Web Technologies: JavaScript, Java, AJAX, HTML, XML, XSL, CSS
    - Code Quality Tools: Fortify, AppScan, JSLint or similar
- Raise key technical/process/risk issues and takes initiative to balance better/faster with secure ways of achieving desired outcomes
- Excellent problem solving & troubleshooting skills
- Excellent written and oral communication skills with ability to adjust to technical and non-technical audiences
- Passion for learning with a track record of acquiring new skills and technologies in a rapid fashion

Preferred:

- Knowledge of in the OWASP top 10 and related exploitation techniques, including but not limited to cross-site scripting, SQL injections, session hijacking and buffer overflows to obtain controlled access to target systems
- Knowledge of the software development lifecycle in a large enterprise environment including agile processes and practices
- Experience with performing manual and automated code review and develop/propose/enforce secure coding standards and policies
- Good Understanding of various web application architectures and web technologies (Java, MS .NET etc.)
- Experience in application firewalls, and intrusion prevention systems (e.g. Mod security) Experience with commercial application scanning tools (DAST) like IBM's AppScan, HP’s WebInspect, etc.
- Experience with commercial static analysis tools (SAST) like HP’s Fortify, Klockworks etc.
- In-depth knowledge of any proxying and/or fuzzing tools such as Paros, Burp, WebScarab, OWASP ZAP etc.
- Familiar with WebServices technologies like XML, SOAP, and AJAX.
- Understanding of server and client side application development, Middleware software’s (Oracle’s WebLogic, IBM’s WebSphere, Apache Tomcat)
- Proficiency in utilization of information security tools such as Nmap, Nessus, Burp Suite, Kismet, and Metasploit; manual techniques to exploit vulnerabilities in networks and applications.
- Industry Training and Certifications:

- ISC^2:
  - Certified Information Systems Security Professional (CISSP)
  - CSSLP - Certified Secure Software Lifecycle Professional (CSSLP)
- SANS:
  - GIAC Secure Software Programmer-Java (GSSP-Java)
  - GIAC Secure Software Programmer- .NET (GSSP-.NET)
  - GIAC Certified Web Application Defender (GWEB)

- Leading technical change in a nonhierarchical environment
- Content management / page publishing systems usage
- Development of web applications with an ad-based revenue model
- Integrating front end code with Java technology stacks
- Automation tools for building of front end assets
- Hands on experience with the following technologies:

  - Web Technologies: JSP, Adobe Experience Manager/CQ
  - Build Tools: Node.JS, Grunt
  - Version Control: Git, SVN
  - OS: Windows, OS X, iOS, Android, Linux/Unix
  - Cloud services: AWS/EC2, Azure, Google, CloudFront, S3, Akamai

- Mobile web-based development and optimization

Education and Certification Requirements:

Bachelor's degree or equivalent experience in a computer science, information systems, engineering, or other related field. Relevant and current industry certifications in information security, cybersecurity and risk management.

CyberSecurity for Hire, LLC is an Equal Opportunity/Affirmative Action employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, national origin, disability or protected veteran status, or any other legally protected basis, in accordance with applicable law.