## Senior Software Security Engineer

Security is a core value at our company and safeguarding sensitive customer information is critical to our continued success. This position is responsible for building a world-class program that embeds security into every aspect of the development process, integrates automated security testing, and maintains an ongoing security training and certification process for staff members.

**Responsibilities**

* Build an industry-competitive domain security lead program to embed security expertise within each scrum team.
* Integrate automated security testing (including both static and runtime) capabilities into an evolving CI/CD program.
* Update, maintain, and deploy new training programs for new hires, annual certification, and expert-level developers (including brown bag lunch-and-learns).
* Develop and deliver consistent automated metrics covering 20+ aspects of the software security program.
* Support architecture review, threat modeling, code review, and other security-related activities throughout the Agile SDLC.
* Coordinate activities related to the bug bounty program, including emergency patching.
* Develop and deliver internal events, including hackathons.
* Develop security-related aspects of the application asset inventory program.
* Maintain development standards, policies, and procedures.

**Qualifications**

* Excellent communication skills and organizational savvy.
* BS in Computer Science or similar technical field.
* 5+ years experience delivering application security programs.
* Expert understanding of production engineering with PHP and/or other popular technologies (development experience a must).
* 2+ years experience supporting mobile application development (iOS, Android, Windows).
* 2+ years experience integrating security activities into Agile development processes.
* Strong knowledge of development tools and services including JIRA, Confluence, GitHub, Stash, and Jenkins.
* Scala and Node.js experience earn bonus points.
* Strong familiarity with multiple software security paradigms including MSSDL, BSIMM, and CSSLP.
* Conference presentation experience at major security events such as OWASP USA or Black Hat/DEFCON.
* Experience with both consulting and leading corporate programs preferred.
* Working knowledge of all vulnerability classes on the OWASP Periodic Table of Vulnerabilities.
* Basic familiarity with virtualization and containerization models.
* Basic understanding of operational security principles, including network security, patch management, and DLP.