Application Security Engineer

Roles and Responsibilities

- Build, deploy, and support large, best-in-class, enterprise-level information security solutions
- Protect the confidentiality, integrity, and availability of all Williams-Sonoma information assets
- Establish security best processes and practices for our mobile, on-premise, and cloud-based platforms
- Provide expert knowledge and guidance to the product teams about security vulnerabilities and remediation controls
- Implement secure Software Security Development Lifecycle processes and software maturity model
- Perform architectural risk analysis and threat modeling, secure design, and source code review
- Conduct security assessments, security testing, and validation of vulnerability scan results. Incorporate security tools/tasks to automate product development and deployment
- Establish supply chain security process and ensure 3rd party software meets the standard
- Mentor and train development teams on secure coding standards and techniques
- Analyze existing security processes to identify opportunities for improvement and make recommendations based on analysis
- Perform security risk assessments
- Help train associates, contractors, alliance, or other third parties on information security policies and procedures
- Perform other responsibilities and duties as assigned

Skills and Qualifications

- BS or MS in Business, Computer Sciences, Engineering, or related field (an equivalent combination of related education, training, and experience may be considered)
- Minimum of 5 + years related work experience

Required Skills

- Deep understanding of security principles
- Expertise with SANS and ISCC2 program
- Expertise in Secure Software Lifecycle
- Expertise with mobile code, malicious code, and anti-virus software
- Experience with cloud security configurations (Azure/O365, AWS, etc.)
- Basic scripting skills in Python, Perl, TCL, Chef/Puppet or Go a plus
- CISSP or equivalent industry certification
- In-depth knowledge of web and mobile security vulnerabilities, attack vectors, and mitigation techniques
- Demonstrated security experience with Mobile (IOS and Android) platforms
- Experience with cloud security, Fortify
- Experience with multiple programming languages (Java, JavaScript, Go, Python, JavaScript X-practices, OWASP Top 10)
- Hands-on level coding experience with at least one scripting and one objected oriented programming language
- Familiarity with tools like Git, Jenkins, CircleCI, Maven, Ant, Gradle, Nexus, SonarQube, Artifactory, Chef, Splunk
- Familiarity with industry trends in the information security space
- US Citizen or Permanent Resident
- Must be fluent in English, both written and spoken