INFORMATION SECURITY ANALYST – APPLICATION & WEB SECURITY

Dillard's is seeking an Information Security Analyst in Little Rock, Arkansas.

Dillard's is seeking an Information Security Analyst to lead the practice of Application Security in Little Rock, Arkansas. As an Information Security Analyst, you will be responsible for leading the team in the discipline of Application and Web Security, including serving as a security consultant for Information Technology. You will advise business process owners, functional area representatives, and other IT personnel on the information security risks within their respective areas of responsibility and help to architect end-to-end solutions with an Application Security focus. There are other responsibilities included with this role that relate to other Security disciplines such as Endpoint Security, Penetration Testing, Network Security and Event Correlation.

ROLES and RESPONSIBILITIES

- Inspect and assess current solutions on Application Security risks.
- Identify security flaws in application code and web configurations, suggest and oversee remediation.
- Create effective SIEM rules and other tools' alerts to notify staff of application and web threats and correlate across environments.
- Lead the vulnerability practice of scanning static and dynamic code across technology stacks and languages.
- Validate risks and vulnerabilities and rate criticality and urgency.
- Conduct penetration tests on code and web environments after every significant modification.
- Ensure security controls are in compliance with applicable laws, regulations and policies to minimize risk and audit findings.
- Architect/design security controls and analysis processes.
- Train others on the team in application security concepts and educate developers on risk based coding including the OWASP best practices.
- Identify areas where IT processes need to be established or improved.
- Participate in on call rotation across the Information Security group.

QUALIFICATIONS and EXPERIENCE

- Authorization to work in the United States without sponsorship.
- Experience analyzing risk in accordance with regulations including PCI, HIPAA, and Sarbanes-Oxley.
- Experience creating processes, procedures and solutions that reduce technical risk and increase operational efficiency.
- Knowledge of web architectures (WebSphere, Apache, IIS/IHS, CDN, NFS mounts, ESB, Jenkins) and application languages (.NET, Groovy, Java, PHP, BASH, Python, AJAX, Ruby on Rails, REST, XML, SOA, HTML, XML, COBOL), and code repositories (GIT, CVS, etc.).
- Understanding of security threats and solutions for applications.
- Ability to work independently and in teams, while meeting multiple deadlines.
- Strong interpersonal and communication skills with proven decision making skills.
- Desire to troubleshoot and lead investigations.
- History of and commitment to ethical behavior and ethical full disclosure.
- Background in several of the following areas: cyber security, intrusion detection/prevention, OS architecture, malicious network traffic identification, malicious code detection/prevention, security auditing, security architecture, security awareness education, databases, identity management, PKI, encryption methods/standards, event correlation, authentication services, advanced incident handling and forensics best.