Application Security Analyst

Description: Cassidy Consulting Group is seeking an Application Security Analyst. This is a W-2 job opportunity. Please visit our website to learn more about Cassidy Consulting Group – https://www.cassidyconsulting.us.

Position Description:
The Application Security Analyst will be responsible for reviewing and identifying security risks in our software scans provided by customers. This role involves conducting security assessments, analyzing code for vulnerabilities, and collaborating with development teams to recommend effective security measures. The successful candidate will contribute to enhancing our application security practices and ensuring the protection of sensitive data. This candidate will be collaborating directly with CRM's, Customers and Customer System Integrator's to communicate open vulnerabilities and understand any false positives reported by customers.

Position Requirements:
- Proven experience in application security, including vulnerability assessments and code reviews.
- Perform regular security assessments of applications through code reviews and vulnerability assessments.
- Analyze and interpret security scan results, identifying vulnerabilities, security risks, and validating reported false positives.
- Analyze and interpret security scan results, identifying and reporting vulnerabilities for remediation.
- Collaborate with development teams to implement secure coding practices and provide guidance on addressing security findings.
- Monitor and respond to security incidents related to applications.
- Collaborate with the incident response team to investigate and mitigate security breaches.
- Stay up-to-date with the latest security threats, vulnerabilities, and industry best practices.
- Contribute to the development and improvement of application security policies and procedures.
- Ensure that applications comply with relevant security standards and regulations.
- Keep abreast of changes in security regulations and update security measures accordingly.
- Stay up-to-date with the latest security threats, vulnerabilities, and industry best practices.
- Contribute to the development and improvement of application security policies and procedures.

Required Skills:
- Bachelor’s degree in computer science, Information Security, or a related field.
- 1-3 years of experience in application security or a similar role.
- Experience with SAST (Fortify, Checkmarx, SonarQube…) and DAST (WebInspect, Burp Suite….) tools
- Proficiency in programming languages such as Java, Python, C++, C#, or others.
- Knowledge of web application security principles and common vulnerabilities.
- Familiarity with security frameworks and compliance standards (e.g., OWASP, NIST, ISO 27001).
- Understanding of secure coding practices and the OWASP Top 10.
- Strong analytical and problem-solving skills.
- Effective communication and collaboration abilities.
- Strong analytical and problem-solving skills.

Desired Skills:
- Relevant certifications such as CompTIA Security+, Certified Ethical Hacker (CEH), or similar.
- Knowledge of cloud security concepts (AWS, Azure, or GCP).
- Familiarity with scripting languages (Python, Ruby, etc.).
- Knowledge of container security (Docker, Kubernetes).

Education: Masters +10yrs or Bachelors +12rs

Security Clearance: DOD Secret (Fully Adjudicated), as a minimum

Location: Radford, VA

Citizenship: United States

Cassidy Consulting Group is an Equal Employment Opportunity employer. Cassidy Consulting Group prohibits discrimination against employees and qualified applicants for employment on the basis of race, color, religion, sex (including pregnancy), age, disability, marital status, national origin, veteran status, or any other classification protected by applicable discrimination laws.