Security Software Engineer Job Profile

Job Objective: To secure and develop robust software solutions, implement advanced security protocols, and conduct thorough vulnerability assessments, leveraging expertise in secure coding practices, cryptography, and network security to protect sensitive data and build resilient systems against evolving threats.

Requirements:

- **Experience:** Minimum 6 years of progressive experience in cybersecurity software engineering, including designing, developing, and implementing secure software solutions.
- **Education:** Master's degree in Cybersecurity or a related field (e.g., Computer Science, Software Engineering) or equivalent practical experience. A Bachelor's degree in Computer Science or a closely related discipline is essential.
- **Technical Skills:**
  - Strong understanding and application of Secure Coding principles (e.g., OWASP Top 10).
  - Expertise in Cryptography (AES, RSA, Hashing).
  - Proficiency in Network Security (Firewalls, IDS/IPS, Nmap, Wireshark).
  - Experience with Penetration Testing, Vulnerability Assessment, and Threat Modeling.
  - Knowledge of Identity and Access Management (IAM), OAuth2, OpenID Connect, and JWT.
  - Proficiency in programming languages such as Python, Java, and Node.js.
  - Experience with Linux, Docker, and Git.
  - Familiarity with SIEM tools (e.g., Splunk) and security auditing.
  - Understanding of compliance requirements (e.g., GDPR, HIPAA).
- **Tools/Software Proficiency:** VS Code, Eclipse, Nessus, Acunetix, VeraCode, SonarQube, Jira, Burp Suite, Metasploit.
- **Soft Skills:** Analytical thinking, risk assessment, problem-solving, attention to detail, strong ethical conduct, and effective communication.
- **Certifications (Highly Valued):** CompTIA Security+, Certified Ethical Hacker (CEH).

Functions and Responsibilities:

- Design, develop, and implement secure software solutions and features for enterprise applications.
- Conduct comprehensive static (SAST) and dynamic (DAST) application security testing to identify and remediate vulnerabilities.
- Develop and integrate secure authentication and authorization mechanisms (e.g., OAuth2, OpenID Connect).

- Create custom security tools and scripts for automated penetration testing and threat detection.
- Enforce security policies and traffic filtering, potentially through secure API gateways.
- Advise development teams on secure coding best practices and provide security awareness training.
- Implement robust data encryption platforms, ensuring data security at rest and in transit.
- Ensure robust logging and auditing features for regulatory compliance (e.g., GDPR, HIPAA).
- Participate in incident response activities, including analyzing security breaches and implementing countermeasures.
- Manage access controls and permissions for sensitive data systems.