Application Security Engineer (AppSec)

Security | SMB | Enterprise

[Company Name] is looking for an Application Security Engineer to help us build secure software from the ground up. You will work alongside development teams to identify and remediate security vulnerabilities, conduct threat modeling, and integrate security tooling into our CI/CD pipelines. This role is both technical and collaborative -- you will be a trusted advisor to engineering teams, helping them ship features quickly without compromising on security.

Key Responsibilities

- Perform security code reviews and design reviews for new features and architecture changes
- Conduct threat modeling sessions with engineering teams to identify and mitigate risks early
- Integrate and manage SAST, DAST, SCA, and secret scanning tools in CI/CD pipelines
- Triage and prioritize vulnerability findings, and work with developers on effective remediation
- Develop and maintain secure coding guidelines, libraries, and reusable security patterns
- Lead or support penetration testing and security assessments of web and API applications
- Champion a security-aware engineering culture through training, documentation, and mentorship

Required Skills & Experience

- 3+ years of experience in application security or software engineering with a security focus
- Deep understanding of common web vulnerabilities (OWASP Top 10) and how to prevent them in code
- Experience with security testing tools: SAST (Semgrep, SonarQube), DAST (Burp Suite, OWASP ZAP), SCA (Snyk, Dependabot)
- Proficiency in at least one programming language used in production (Python, Java, Go, JavaScript/TypeScript)
- Experience with authentication and authorization protocols (OAuth 2.0, OIDC, SAML, JWT)
- Familiarity with CI/CD security integration and DevSecOps practices
- Strong communication skills to explain security risks to technical and non-technical audiences

Nice-to-Have

- Experience with cloud security (AWS, GCP, or Azure IAM, networking, and service configurations)
- Security certifications such as OSCP, GWAPT, CEH, or CSSLP
- Experience with container and Kubernetes security (pod security, network policies, image scanning)
- Bug bounty participation or responsible disclosure experience
- Background in compliance frameworks (SOC 2, ISO 27001, PCI-DSS)

Tech Stack

Burp Suite | Semgrep | Snyk | SonarQube | OWASP ZAP | GitHub Advanced Security | Terraform | Docker | Kubernetes | Python

What We Offer

- Competitive salary and equity package
- Flexible remote or hybrid work arrangement
- Health, dental, and vision insurance
- Annual learning and development budget
- Generous PTO policy

Interview Process

1. Recruiter phone screen (30 min)
2. Technical phone screen covering web security fundamentals and secure coding (45 min)
3. Practical exercise: security code review or threat modeling session (60 min)
4. On-site or virtual loop: architecture security review, vulnerability analysis, and team fit (3 hours)
5. Final conversation with the security team lead or CISO