Security Engineer

Security | SMB | Enterprise

We are looking for a Security Engineer to protect [Company Name]'s systems, data, and customers. You will work across application security, infrastructure security, and compliance to identify vulnerabilities, build defensive systems, and embed security practices into our development lifecycle. This role partners closely with engineering, DevOps, and product teams to make security an enabler rather than a blocker.

Key Responsibilities

- Conduct application security assessments including code reviews, penetration testing, and threat modeling
- Design and implement security controls for cloud infrastructure (IAM policies, network segmentation, encryption)
- Build and maintain security monitoring and alerting using SIEM and intrusion detection systems
- Lead vulnerability management — triage, prioritize, and drive remediation of security findings
- Develop and maintain security policies, standards, and incident response playbooks
- Support compliance efforts (SOC 2, ISO 27001, GDPR, HIPAA) by implementing technical controls and providing audit evidence
- Champion security awareness across the engineering organization through training and secure coding guidelines

Required Skills & Experience

- 3+ years of experience in Security Engineering, Application Security, or Infrastructure Security
- Hands-on experience with penetration testing and vulnerability assessment tools (Burp Suite, OWASP ZAP, Nessus)
- Strong understanding of OWASP Top 10 and common web application vulnerabilities
- Experience securing cloud environments (AWS, GCP, or Azure) including IAM, VPC security, and encryption
- Proficiency in at least one programming or scripting language (Python, Go, or Bash) for automation
- Knowledge of network security concepts (firewalls, IDS/IPS, DDoS mitigation, TLS/mTLS)
- Familiarity with at least one compliance framework (SOC 2, ISO 27001, GDPR, or HIPAA)

Nice-to-Have

- Security certifications (CISSP, CEH, OSCP, or AWS Security Specialty)
- Experience with DevSecOps practices — integrating SAST/DAST into CI/CD pipelines
- Bug bounty program management experience
- Knowledge of container security (Falco, Trivy, Aqua Security)
- Incident response and digital forensics experience

Tech Stack

Burp Suite | OWASP ZAP | Snyk | SonarQube | AWS Security Hub | Splunk | Terraform | Falco | HashiCorp Vault | Trivy

What We Offer

- Competitive salary and equity at [Company Name]
- Security certification sponsorship and conference attendance budget
- Flexible remote or hybrid work arrangements
- Dedicated time for security research and open-source contributions
- Comprehensive health, dental, and vision insurance
- Generous PTO and mental health days

Interview Process

1. Recruiter phone screen (30 min)
2. Technical conversation with Security team lead — discuss security experience and approach (45 min)
3. Hands-on exercise: identify vulnerabilities in a sample application or review a cloud security configuration (60 min)
4. Threat modeling session: walk through designing security for a new feature or system (45 min)
5. Culture fit and values conversation with hiring manager (30 min)
6. Optional: meet the broader security team