Cloud Security Engineer

Security | SMB | Enterprise

[Company Name] is looking for a Cloud Security Engineer to protect our cloud infrastructure and ensure our environments meet the highest security standards. You will design and enforce IAM policies, harden cloud configurations, build automated compliance monitoring, and respond to security events across our cloud platforms. This role is ideal for someone who combines deep cloud platform expertise with a security-first mindset.

Key Responsibilities

- Design and implement IAM policies, roles, and permission boundaries across cloud accounts
- Harden cloud configurations using CIS benchmarks and industry best practices
- Build and maintain automated compliance monitoring and alerting pipelines
- Investigate and respond to cloud security incidents including unauthorized access and data exposure
- Conduct security reviews of cloud architecture designs and Terraform / CloudFormation templates
- Manage cloud-native security tools including GuardDuty, Security Hub, Defender for Cloud, or Security Command Center
- Collaborate with DevOps teams to implement least-privilege access and network segmentation

Required Skills & Experience

- 3+ years of experience in cloud security or cloud engineering roles
- Deep expertise with at least one major cloud platform (AWS, Azure, or GCP) security services
- Strong knowledge of IAM design including roles, policies, service accounts, and cross-account access
- Experience with cloud security posture management (CSPM) tools
- Proficiency with infrastructure-as-code (Terraform, CloudFormation) and reviewing templates for security issues
- Understanding of network security in cloud environments (security groups, NACLs, private endpoints)
- Familiarity with logging and monitoring tools (CloudTrail, Azure Monitor, or GCP Audit Logs)
- Knowledge of compliance frameworks relevant to cloud (SOC 2, CIS Benchmarks, NIST)

Nice-to-Have

- Cloud security certifications (AWS Security Specialty, CCSP, Azure Security Engineer Associate)
- Experience with multi-cloud security strategies
- Knowledge of Kubernetes security (RBAC, network policies, pod security standards)
- Familiarity with SIEM platforms (Splunk, Sentinel, Chronicle) for cloud log analysis
- Experience with cloud forensics and incident response playbooks

Tech Stack

AWS IAM | Terraform | AWS GuardDuty | AWS Security Hub | Prisma Cloud | CloudTrail | Kubernetes

Prowler ScoutSuite

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) — role fit and logistics
2. Technical phone screen (45 min) — cloud security fundamentals and IAM design
3. Architecture exercise — design a secure multi-account cloud landing zone
4. On-site or virtual loop (3 hours) — incident response scenario, policy review, and team fit
5. Offer and reference checks