SAM HOWARD

Senior Cloud Engineer — Platform, DevOps & Site Reliability

Huntsville, AL (open to fully remote) · samhoward1227@gmail.com · linkedin.com/in/samhoward-cloud · samhoward.cloud

Cloud infrastructure engineer building and securing AWS and GCP platforms. Cut a client's AWS bill about 87% (roughly $156K/year) through cost-governance automation. Ships production Kubernetes, Terraform, and CI/CD, with unusual depth in workload identity and compliance-heavy environments (NIST 800-53, zero trust, FedRAMP-adjacent). Led a 10-person engineering team. Active TS/SCI clearance.

Experience

Deloitte — Senior Cloud Engineer

Apr 2024 – Present

- Cut a client's AWS bill about 87% (roughly $156K/year) in 12 months by building cost governance into the platform: instance right-sizing, automated non-production scheduling, reserved capacity, and S3 lifecycle policies.
- Owned GitLab CI/CD as the only path to production, unblocking delivery teams and debugging containerized pipeline failures across EKS, Lambda, S3, and Systems Manager.
- Containerized ML models and ran them as production workloads on EKS, GCP, and Snowflake, adapting the deployment path to each environment.
- Led the migration of Jira, Splunk, and Keycloak into managed services as the primary technical resource, and decommissioned the legacy instances.
- Built Python observability tooling that restored web-traffic attribution lost to VPN egress, shipped as both a desktop GUI and a headless binary.

COLSA — Security Operations Technical Lead

Mar 2022 – Apr 2024 · Promoted from Security Analyst in 11 months

- Led a 10-person team monitoring network and cloud traffic for roughly 130 customer sites worldwide, on 24/7 coverage.
- Held a zero-miss record on confirmed true-positive detections over 12 months, catching incidents that parallel teams missed.

- Drove customer sites through federal security readiness audits, raising pass rates from 62% to 85%.
- Hired, trained, and certified junior analysts, and owned the team's end-of-training technical assessments.
- Built the monthly security posture reporting in Tableau and ran vulnerability management with Tenable across the customer estate.

Hexagon — Lead Support Analyst

Oct 2020 – Feb 2022 · Promoted from Help Desk Analyst in 6 months

- Took over chat support operations solo within 6 months, trained new analysts, and improved response-time efficiency 30%.

Selected Projects

Zero-Trust Workload Identity on Kubernetes

Report · Code and evidence (DOI) · GitHub

- Built a SPIFFE/SPIRE workload-identity control plane on Amazon EKS in a VPC with no internet gateway and no NAT, replacing long-lived static credentials with X.509 SVIDs on a one-hour TTL. Rebuilds from an empty AWS account in about 30 minutes.
- Implemented two-tier attestation (EC2 node, then workload via Kubernetes projected service-account tokens) so pods pull identity over the Workload API with no secrets on disk and rotate under live traffic without restarts.
- Enforced mutual TLS verified at the handshake record by peer SPIFFE ID, so a workload with a valid certificate but an unauthorized identity is refused by name.
- Built Go workloads with GOFIPS140 against a FIPS 140-3 validated module (CMVP #5247); the build fails rather than shipping an image that only appears FIPS-enabled.
- Ran the signing CA on a non-exportable KMS key with a policy that survives Terraform replacing the IAM role it names, and shipped audit telemetry to CloudWatch with alarms on sustained identity denials.

Event-Driven Media Pipeline (production SaaS replacement)

emilynovellagalleries.com

- Replaced a stack of paid SaaS subscriptions with a custom delivery platform: a headless Raspberry Pi appliance compresses and uploads multi-gigabyte galleries to S3, with spoken progress via AWS Polly and an offline fallback.
- Architected an S3-triggered container-image Lambda that unzips payloads, generates thumbnails, and builds gallery pages, with mappings in DynamoDB and archives aged to Glacier after 30 days.
- Gated per-gallery access with CloudFront signed cookies and SHA-256 hashed keys stored without plaintext; penetration testing confirmed full tenant isolation.

Serverless Portfolio Platform

Source on GitLab

- Private S3 origin behind CloudFront with Origin Access Control, ACM-managed TLS, and Route 53 DNS, declared entirely in modular Terraform and reproducible from a single apply.
- GitLab pipeline that plans infrastructure changes, gates applies behind manual approval, syncs assets, and invalidates the CDN cache on every push to main. No console operations in the deploy path.

Technical Skills

Cloud: AWS (EKS, ECS, Lambda, S3, DynamoDB, CloudFront, Route 53, IAM, VPC, KMS, API Gateway, ACM, Systems Manager), GCP (GKE, Cloud Functions, GCS), Azure, GovCloud

Platform & Infrastructure as Code (IaC): Terraform, Ansible, Kubernetes, Docker, Helm, GitLab CI/CD, GitHub Actions, CI/CD pipeline design, Python, Go, Bash, Linux

Security: Zero-trust architecture, SPIFFE/SPIRE workload identity, mTLS, KMS and PKI, IAM design, NIST 800-53 / 800-207, FedRAMP, SOC 2, FIPS 140-3, penetration testing, Tenable

Observability & Operations: Prometheus, Grafana, CloudWatch, Splunk, Site Reliability Engineering (SRE), FinOps and cloud cost optimization

Data: Snowflake, Databricks, Tableau, ETL pipelines, MLOps

Education & Certifications

M.S. Cybersecurity — Georgia Institute of Technology · Aug 2023 – Dec 2026

B.S. Information Technology, Cum Laude — Liberty University

Certifications: AWS Certified Solutions Architect – Associate · CompTIA PenTest+ · CompTIA CySA+ · CompTIA Security+

Clearance: Active TS/SCI