SAM HOWARD

Senior Cloud Security Engineer — Regulated Cloud Infrastructure

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

Cloud engineer who builds and secures AWS and GCP infrastructure under external audit. Four years operating inside regulated control frameworks, including taking customer environments through external compliance audits and raising pass rates from 62% to 85%. Cut a client's AWS bill about 87% (roughly $156K/year) through cost-governance automation. Deep in workload identity and secrets elimination: replaced long-lived static credentials with short-lived, auto-rotating certificates on production Kubernetes, with the control evidence to back it.

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 storage lifecycle policies.
- Owned GitLab CI/CD as the only path to production across EKS, Lambda, and S3, enforcing a deploy path with no manual console changes and a full audit trail on every release.
- 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, including the identity and access layer, and decommissioned the legacy instances.
- Built Python observability tooling that restored 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 running 24/7 monitoring of network and cloud traffic across roughly 130 customer sites worldwide.
- Prepared customer environments for external regulatory audits and drove pass rates from 62% to 85% through enforced remediation and evidence collection.
- Held a zero-miss record on confirmed true-positive detections over 12 months, catching incidents that parallel teams missed.
- Ran vulnerability management with Tenable across the estate and built monthly security posture reporting in Tableau for executive stakeholders.
- Hired, trained, and certified junior analysts, and owned the team's end-of-training technical assessments.

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

- Eliminated long-lived static credentials from a production Kubernetes environment, replacing them with X.509 SVIDs on a one-hour TTL issued through SPIFFE/SPIRE. Credentials rotate under live traffic with no restarts and no secrets on disk.
- Ran the whole control plane in a VPC with no internet gateway and no NAT, on an air-gapped supply chain of 16 images with no dependency on any registry outside AWS. Rebuilds from an empty account in about 30 minutes.
- Enforced mutual TLS verified at the handshake by peer identity, so a workload holding a valid certificate but an unauthorized identity is refused by name. Service-to-service authorization is an allowlist, not a network boundary.
- Ran the signing CA on a non-exportable KMS key and built workloads against a FIPS 140-3 validated cryptographic module, with the build failing rather than shipping an image that only appears compliant.

- Produced a control-mapping toolkit tying each capability to specific framework controls (identity, authenticator management, transit encryption, least privilege, audit), with CloudWatch audit telemetry, retention, and alarms on sustained identity denials. The point was auditable evidence, not just a working system.

Event-Driven Media Pipeline (production, multi-tenant)

emilynovellagalleries.com

- Built a multi-tenant delivery platform replacing paid SaaS: event-driven ingestion to S3, a container-image Lambda that processes payloads and generates per-tenant pages, mappings in DynamoDB, and archives aged to cold storage after 30 days.
- Gated per-tenant access with CloudFront signed cookies and SHA-256 hashed keys stored without plaintext. Penetration testing confirmed full isolation between tenants.

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. Change control enforced in the pipeline, not by policy document.

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

Security: Zero-trust architecture, workload identity (SPIFFE/SPIRE), secrets management and elimination, mTLS, KMS and PKI, IAM and least-privilege design, encryption in transit and at rest, penetration testing, Tenable

Governance, Risk & Compliance: SOC 2, PCI DSS, SOX ITGC concepts, FIPS 140-3, NIST 800-53 / 800-207, external audit preparation and evidence collection, change control, separation of duties

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

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