SAM HOWARD

Senior Cloud Engineer — Federal Cloud, Zero Trust & Platform Security

Huntsville, AL · samhoward1227@gmail.com · linkedin.com/in/samhoward-cloud · samhoward.cloud

Active TS/SCI Clearance · AWS Certified Solutions Architect – Associate

Cloud infrastructure engineer with an active TS/SCI clearance, working across IT, cybersecurity, and cloud. Builds secure, cost-efficient AWS and GCP infrastructure inside DoD networks and federal ATO boundaries. Cut client AWS spend about 87% (roughly $156K/year) through cost-governance automation. Led a 10-analyst CSSP team covering about 130 DoD sites. Hands-on depth in Kubernetes, Terraform, Python, SPIFFE/SPIRE workload identity, and RMF control implementation.

Experience

Deloitte — Senior Cloud Engineer

Apr 2024 – Present

- Cut client AWS spend about 87% (roughly $156K/year) in 12 months through cost-governance automation: right-sizing, non-production scheduling, reserved capacity, and S3 lifecycle policies.
- Served as the primary technical resource on the migration of Jira, Splunk, and Keycloak into managed environments, and decommissioned the legacy instances.
- Maintained GitLab CI/CD as the sole path to production, unblocking delivery teams and resolving 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.
- Built Python monitoring tooling for a government client that restored web-traffic attribution obscured by VPN usage, shipped as both a GUI and a headless executable.

COLSA — C5ISR CSSP Technical Lead

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

- Led 10 analysts monitoring network and cloud traffic across roughly 130 DoD subscriber sites, CONUS and OCONUS.
- Held a zero-miss record on true-positive detections over 12 months, including detections missed by parallel teams.
- Coordinated internal and subscriber-site teams to stand up full CSSP capabilities, raising CCRI pass rates from 62% to 85%.
- Provided technical guidance and training to junior analysts and administered JQR end-of-training certification exams.

Cyber Analyst I

- Authored monthly Argus security posture reports in Tableau, compiling critical CTO alarms and snapshots for site leadership.
- Drove ACAS vulnerability findings down far enough through enforced remediation that the team tightened its own reporting thresholds to sustain coverage.
- Enforced ARCYBER Cyber Tasking Orders by reporting vulnerable assets to sites and quarantining affected systems.

Hexagon — Lead Chat Analyst

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

- Moved from phone support to running chat operations solo within 6 months, training new analysts and improving response-time efficiency 30%.

Projects

Zero-Trust Workload Identity for Federal Cloud-Native Environments

Georgia Tech practicum · Report · Code and evidence (DOI)

- Designed and deployed a SPIFFE/SPIRE workload-identity control plane on Amazon EKS inside a VPC with no internet gateway and no NAT, emulating a restricted federal enclave. Rebuilds from an empty AWS account in about 30 minutes.
- Replaced long-lived static credentials with X.509 SVIDs on a one-hour TTL, issued through two-tier attestation: EC2 node first, then workload via Kubernetes projected service-account tokens. No secrets on disk; credentials rotate under live traffic with no restarts.

- Demonstrated mutual TLS at the handshake record, carrying peer SPIFFE ID, negotiated protocol, and cipher. A workload holding a valid SVID with an unauthorized identity is refused by name.
- Built Go workloads with GOFIPS140 against the Go Cryptographic Module (CMVP #5247) so the handshake runs inside a FIPS 140-3 validated module; the build fails rather than shipping an image that only appears FIPS-enabled.
- Generated the signing CA key in KMS as non-exportable, with a key policy that survives Terraform replacing the IAM role it names.
- Built an air-gapped supply chain of 16 images with no dependency on a registry outside AWS, and shipped SPIRE audit and workload events to CloudWatch with retention, metric filters, and an alarm on sustained identity denials.
- Mapped the resulting capabilities to NIST SP 800-53 controls (IA-5, IA-9, SC-8, SC-12, SC-13, AC-3, AC-6, AU-2, AU-9), aligned to NIST SP 800-207, CISA's Zero Trust Maturity Model, and OMB M-22-09, to evidence RMF/ATO compliance without static secrets.

Event-Driven Hybrid-Cloud Media Pipeline

In production at emilynovellagalleries.com

- Built a headless Raspberry Pi appliance (systemd daemon) that detects an inserted USB drive, compresses galleries over 7 GB, and uploads them to S3, reading progress aloud through AWS Polly with an offline espeak fallback.
- Architected an S3-triggered container-image Lambda that unzips the payload, generates thumbnails, and builds a lazy-loading gallery page, with mappings tracked 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 the plaintext. Penetration testing confirmed full isolation between client galleries.

Serverless Portfolio Platform

Source on GitLab

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

Education & Certifications

M.S. Cybersecurity, Public Policy track — Georgia Institute of Technology · Aug 2023 – Dec 2026

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

Certifications: AWS Certified Solutions Architect – Associate (2026–2029) · CompTIA PenTest+ (2025–2028) · CompTIA CySA+ (2022–2028) · CompTIA Security+ (2021–2028)

Technical Skills

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

Security & Compliance: Zero-Trust Architecture, SPIFFE/SPIRE workload identity, mTLS, PKI, IAM design, NIST SP 800-53 / 800-207, Risk Management Framework (RMF), ATO support, FedRAMP, SOC 2, CISA Zero Trust Maturity Model, FIPS 140-3, ACAS, Tenable, Azure Sentinel, Kibana

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

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

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