SAM HOWARD

Lead Cloud Engineer | Active U.S. Security Clearance

samhoward1227@gmail.com samhoward.cloud linkedin.com/in/samhoward-cloud gitlab.com/samhoward-cloud-group

PROFESSIONAL SUMMARY

Lead Cloud Engineer with 5+ years across IT, cybersecurity, and cloud and an active U.S. government security clearance, specializing in secure, automated, cost-optimized AWS and GCP infrastructure for highly regulated federal and DoD environments. Promoted into technical leadership at every role—including leading a 10-analyst CSSP team safeguarding ~130 DoD installations—and architects zero-trust, cloud-native systems mapped directly to NIST SP 800-53 / RMF controls. Combines hands-on DevOps (EKS, Kubernetes, Lambda, GitLab CI/CD) with Python automation, MLOps, and zero-trust security engineering.

PROFESSIONAL EXPERIENCE

Deloitte | Cloud Engineer II → Lead Cloud Engineer Apr 2024 – Present

- **Cloud Architecture:** Designed and implemented automated AWS workflows to scale services and shut down or restart resources during off-peak hours, reducing recurring cloud infrastructure costs by more than $120K annually.
- **DevOps & Integrations:** Engineered and resolved integration issues for containerized pipelines using EKS, Lambda, S3, and AWS Systems Manager, driving CI/CD workflows through GitLab.
- **Machine Learning & Data Pipelines:** Built ETL pipelines and supported the implementation of ML models across AWS, GCP, Snowflake, and Databricks environments.
- **Software Engineering:** Developed Python-based monitoring tools for government clients to track VPN usage and website activity, delivering both GUI demonstrations and headless production versions compiled into Windows executables.
- **System Modernization:** Led and supported system transition and decommissioning efforts for Jira, Splunk, and Keycloak into Deloitte-operated environments.

COLSA | Cyber Analyst I → C5ISR CSSP Technical Lead Mar 2022 – Apr 2024

- Promoted from Cyber Analyst I to lead the CSSP team within 11 months of hire.
- Led a team of 10 analysts monitoring and analyzing network and cloud traffic across ~130 DoD subscriber sites (CONUS and OCONUS installations) to identify and mitigate cyber threats.
- Coordinated internal and external teams to leverage full CSSP capabilities and directly assisted subscriber sites in passing their Command Cyber Readiness Inspections (CCRIs).
- Provided technical guidance and training to junior analysts and administered JQR end-of-training certification exams.
- As an analyst, conducted network traffic, security log, and ACAS vulnerability analysis and delivered monthly security posture reports in Tableau.

Hexagon | Help Desk Analyst → Lead Chat Analyst Oct 2020 – Feb 2022

- Promoted within six months from phone support to running online-chat operations solo; trained new analysts and exceeded response-time, quality, and retention targets.

EDUCATION & CERTIFICATIONS

M.S. Cybersecurity | Georgia Institute of Technology Aug 2023 – Present

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

Certifications: CompTIA PenTest+ • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Security+ • Microsoft Certified: Azure Fundamentals

TECHNICAL PROJECTS

Zero-Trust Workload Identity for Federal Cloud-Native Environments

Georgia Tech Practicum

- **Architecture & Deployment:** Designed and deployed a SPIFFE/SPIRE zero-trust workload-identity control plane on Amazon EKS, architected to emulate a restricted U.S. Army “Private Only” cloud environment, replacing long-lived static credentials with short-lived, auto-rotating X.509 SVIDs (~4-hour TTL).
- **Continuous Attestation & mTLS:** Implemented a two-tier attestation pipeline—authenticating EC2 nodes and then workloads via Kubernetes projected service-account tokens (k8s_psat) against the Kubernetes API—so each pod pulls its identity over the Workload API with no secrets on disk, enabling automatic mutual TLS between services.
- **RMF Compliance Translation Toolkit:** Built a framework mapping cloud-native identity capabilities directly to NIST SP 800-53 controls (IA-2, IA-5, SC-8, AC-6, AU-2), aligned with NIST SP 800-207, CISA’s Zero Trust Maturity Model, and OMB M-22-09, to evidence federal RMF/ATO compliance without static secrets.
- **Cloud-Native Troubleshooting & Hardening:** Resolved production-grade edge cases spanning Private-Only VPC DNS/OIDC resolution, default StorageClass/PVC binding, and IRSA-vs-EKS Pod Identity CSI timeouts; defined the production hardening path with FIPS 140-validated crypto, an HSM/KMS-backed upstream CA, and an external high-availability datastore.

Serverless Portfolio Platform — Infrastructure as Code

samhoward.cloud • live

- **Architecture & Delivery:** Designed and deployed a fully serverless portfolio platform on AWS—private S3 origin behind CloudFront with Origin Access Control, ACM-managed TLS, and Route 53 DNS—with the entire stack declared in modular Terraform and reproducible from a single apply.
- **CI/CD Pipeline:** Built a GitLab pipeline that validates and plans infrastructure changes, gates applies behind manual approval, syncs frontend assets to S3, and invalidates the CloudFront cache on every push to main—zero console operations in the deploy path (source code public on GitLab).
- **Serverless Backend & Hardening:** Implemented an API Gateway + Python Lambda contact service persisting to DynamoDB with SES notifications, secured with least-privilege IAM scoped to single resources, request throttling (2 rps), honeypot bot filtering, and full server-side input validation.

Event-Driven Hybrid-Cloud Media Pipeline

emilynovellagalleries.com

- **Full-Stack Photography Platform:** Designed and built a custom site and automated gallery-delivery system for a photography business, replacing costly SaaS subscriptions and insecure USB handoffs with a public portfolio/contact frontend and a private, secure pipeline for distributing finished client galleries.
- **Headless Edge Ingestion:** Engineered a fully headless Raspberry Pi gateway that auto-detects an inserted USB drive, extracts the photo archive, and uploads it to a dedicated S3 bucket—using AWS Polly with an attached speaker to deliver real-time spoken progress updates.
- **Event-Driven Cloud Processing:** Architected an S3-triggered workflow in which Lambda captures the object URI and launches an ECS container that unzips the images and dynamically builds the client’s gallery webpage, then provisions Lambda-generated cryptographic URL and passkey pairs for secure, per-client access.
- **Storage, Tracking & Hardening:** Tracked passkeys and gallery mappings in DynamoDB for retrieval, transitioned galleries to Glacier after 30 days via S3 lifecycle policies, served the site over HTTPS through CloudFront with Route 53 DNS, and conducted penetration testing to verify full isolation of every client gallery.

TECHNICAL SKILLS

- **Cloud & Infrastructure:** AWS (EKS, ECS, Lambda, S3, DynamoDB, Route 53, CloudFront, IAM, VPC, KMS, Systems Manager, API Gateway, SES, ACM), GCP, Azure.
- **Infrastructure as Code & DevOps:** Terraform, GitLab CI/CD, Python, Bash, Linux, ETL pipelines, MLOps, GUI/headless tooling.
- **Containers & Orchestration:** Kubernetes, Docker, Helm, Amazon EKS / ECS.
- **Data & Analytics:** Snowflake, Databricks, Tableau.
- **Security & Compliance:** Zero-Trust Architecture, SPIFFE/SPIRE, mTLS, NIST SP 800-53 / 800-207, RMF, CISA Zero Trust Maturity Model, ACAS, Tenable, Kibana, Azure Sentinel.