

Ian Thomas

AWS Cloud Engineer | Security & FinOps Specialist

 iankthomasllc@gmail.com

 [443-838-1312](tel:443-838-1312)

 Houston, TX

 <https://www.linkedin.com/in/ian-thomas-aws21>

 www.iankthomas.com

Technical Skills

- Cloud Platforms: Amazon Web Services (AWS)
- Cloud Security: Identity & Access Management (IAM), AWS KMS, Infrastructure Hardening, Principle of Least Privilege (PoLP), Zero Trust Architecture, Key Management
- FinOps & Cost Governance: Cloud Financial Management (CFM), AWS Cost Explorer, Rightsizing, AWS Budgets, Savings Plans, Spot Instances, Cost Allocation Tagging
- Compliance & Monitoring: AWS Security Hub, Amazon GuardDuty, AWS CloudTrail, Amazon CloudWatch, AWS Config, CIS Benchmarks compliance auditing
- Network & Data Security: VPC Architecture, Security Groups, Network ACLs (NACLs), Systems Manager (SSM) Session Manager, S3 Lifecycle Policies, S3 Intelligent-Tiering
- Operating Systems & Tools: Linux/Unix CLI, Git, GitHub

Certifications

- AWS Certified Cloud Practitioner
- AWS Certified AI Practitioner
- AWS Certified Solutions Architect
- AWS Certified Security Specialty
- AWS Certified Machine Learning Specialty

Education

Ferris State University	Bachelor's of Science
Integrative Studies	
University of Virginia	Certificate
Cloud Computing	

Experience

Amazon	Katy, TX
Fulfillment / Logistics Specialist (Targeting FinOps & Efficiency)	
05/2024 - Present	
Resource Optimization: Analyzed daily operational volume data to optimize inventory placement, mirroring the core FinOps principles of cloud resource rightsizing and capacity planning. Process Standardization: Authored standard operating procedures for high-velocity workflows, applying the same methodical architecture logic needed to write AWS Service Control Policies (SCPs). Cost Governance Support: Monitored and reported on physical asset usage and operational waste, translating directly to cloud financial management and cost allocation tracking.	
Apple	Towson, MD
Operations / Technical Specialist	09/2023 - 05/2024
Access Control & Security: Enforced strict physical security protocols and inventory access control measures, embodying the core AWS security framework of the Principle of Least Privilege (PoLP). Data Security Auditing: Managed secure device provisioning, tracking, and serialization, applying foundational concepts of data integrity, chain of custody, and cloud asset tagging. Incident Reporting: Utilized internal monitoring software to track, escalate, and log anomalies, matching the daily workflow required for monitoring AWS CloudTrail and Amazon GuardDuty alerts.	
Nearmap	Remote
Solutions Architect	03/2022 - 08/2023
Data Lifecycle Management: Processed large-scale aerial imagery datasets, building a solid understanding of high-volume data ingestion, storage tiers, and retrieval optimization. Quality Assurance Auditing: Conducted precise validation checks on geospatial data pipelines, reflecting the analytical skills required to audit AWS Security Hub compliance frameworks. Infrastructure Familiarity: Collaborated within a data-heavy environment reliant on cloud-scale storage, mapping directly to managing complex Amazon S3 and database workloads.	

Projects

Automated Multi-Account Security Governance Framework

- Designed a multi-account cloud architecture using **AWS Organizations** to isolate development, staging, and production environments.
- Enforced organization-wide **Service Control Policies (SCPs)** to block unauthorized AWS regions and restrict root account access.
- Deployed **AWS Security Hub** to continuously audit infrastructure compliance against **CIS AWS Foundations Benchmarks**.
- Automated real-time threat remediation by linking **Amazon EventBridge** with **AWS Lambda** to instantly disable compromised **IAM** access keys.
- Configured **Systems Manager Session Manager** for secure terminal access to private EC2 instances, eliminating public **Bastion hosts** and port 22 vulnerabilities.

<https://github.com/iankthomas/AWS/tree/Security>

Intelligent FinOps Cost Optimization Engine

- Architected an automated cost monitoring system utilizing **AWS Cost Anomaly Detection** linked to **Amazon SNS** for real-time budget alerts.
- Leveraged **AWS Compute Optimizer** data to automate the rightsizing of over-provisioned compute resources, projecting a 35% reduction in monthly spend.
- Programmed **S3 Lifecycle Policies** and **S3 Intelligent-Tiering** engines to automate data migration to Glacier Deep Archive based on access patterns.
- Structured a hybrid compute strategy blending **Compute Savings Plans** for baseline traffic and **EC2 Spot Instances** for fault-tolerant workloads.
- Enforced mandatory **Cost Allocation Tags** across all resources via automated AWS Config rules to establish clear business unit cost mapping.

<https://github.com/iankthomas/AWS/tree/Security>