Menelik Rowe

Chicago, IL | roweramirez01@gmail.com | (323) 425-3641 | linkedin.com/in/menelikr

Profile

Cloud & DevSecOps Engineer with a cybersecurity foundation, specializing in secure AWS infrastructure, automation, CI/CD pipelines, Terraform/CloudFormation, and Python/Bash scripting. Experienced in designing and deploying CloudFront–OAC architectures, hardening cloud environments, and building developer-ready automation systems. I combine cloud engineering, security best practices, and modern tooling to ship fast, reliable, and secure systems.

CORE SKILLS

Cloud: AWS (CloudFront, S3, Route 53, IAM, OAC/OAI, EC2, Lambda, CloudWatch, SSM)

IaC: Terraform, CloudFormation

DevOps: GitHub Actions, CI/CD pipelines, automation, monitoring/logging

Scripting: Python, Bash, JavaScript

Security: IAM least privilege, WAF tuning, security headers, CSP/HSTS, Linux hardening

Tools: Docker, Git, Linux

Certifications: CompTIA Security+, CySA+, PenTest+, Project+, Network+, A+, Linux Essentials (LPI), ITIL 4

CLOUD & DEVSECOPS PROJECTS

Modern Portfolio Infrastructure – AWS CloudFront + OAC + S3

2024 — 2025

Astro · TypeScript · Tailwind · Terraform · CloudFront · S3 · Route 53 · OAC · GitHub Actions

- Designed and deployed a fully serverless portfolio architecture using **AWS CloudFront**, **Origin Access Control (OAC)**, and a **private S3 bucket** for secure static hosting.
- Implemented security hardening: **CSP**, **HSTS**, **signed requests**, blocked public S3 access, and configured IAM least-privilege roles.
- Automated global distribution and routing using **Route 53**, CloudFront functions, and TLS via ACM.
- Integrated CI/CD using **GitHub Actions** to build Astro site, sync to S3, and auto-invalidate CloudFront cache.
- Added observability using CloudFront logs + S3 log bucket + CloudWatch metrics.
- Built the full architecture diagram and documented the system end-to-end (Infra, networking, delivery, logging, security).

Impact: Reduced hosting cost to near-zero, deployed globally optimized infra, and demonstrated cloud + security + automation skills.

Terraform IaC Lab – Modular AWS Infrastructure

2025

Terraform · AWS · IAM· VPC · EC2 · CloudWatch

- Built modular Terraform configurations for VPCs, subnets, routing, IAM roles/policies, EC2 deployments, and S3 storage.
- Implemented remote state storage and environment-based workspaces.
- Hardened EC2 instances using security groups, IAM least privilege, and system patching workflows.
- Integrated CloudWatch logs and alarms for system visibility.

Python Automation Scripts

2024 — 2025

Python · Bash · Boto3 · API Scripting

- Developed Python scripts leveraging **Boto3** for automating S3 lifecycle policies, CloudWatch log insights, and IAM auditing tasks.
- Built Bash automations for local tooling, environment setup, and CI pipeline utilities.
- Created small internal tools for API testing, log parsing, and infrastructure validation.

React Native Application (In Progress)

Present

React Native · Expo · TypeScript

- Developing cross-platform mobile app with secure API integration, cloud-backed storage, and optimized front-end components.
- Implementing CI via GitHub Actions and integrating cloud services into the app's backend.

EXPERIENCE

Cloud / DevSecOps Engineer, Freelance / Projects

2021 — Present

Designed secure, automated cloud systems across AWS environments.

- Designed and deployed secure AWS architectures using **CloudFront, OAC, S3, Route 53, IAM, Lambda, EC2**, and CloudWatch.
- Implemented **CI/CD pipelines** (GitHub Actions) for code build, test, deployment, and CloudFront cache invalidation.
- Automated infrastructure provisioning using **Terraform and CloudFormation**.
- Applied cloud security best practices: IAM least privilege, WAF tuning, header hardening, encryption policies, and incident response patterns.
- Built internal automations in **Python/Bash** to speed up workflows and reduce manual steps.
- Containerized workloads using Docker and implemented environment consistency across dev/stage.
- Troubleshot Linux-based systems and automated OS-level tasks using Bash/Python.

Cybersecurity Analyst, Cloud Security Lab (Hands-On Scenario)

2022 — 2024

Hands-on lab work in detection, IR workflows, system hardening, and cloud security.

- Analyzed logs, built Splunk detections, and responded to simulated cloud attacks.
- Performed Linux/Windows hardening and secured multiple services (FTP, SMB, SSH, DNS, HTTP).
- Conducted IAM and file-permission audits; remediated privilege exposures.
- Developed reporting workflows and incident analysis playbooks.

Technical Foundation (Career Transition)

2019 — 2023

Transitioned out of BD into cybersecurity and cloud engineering through labs, certs, and daily hands-on practice.

Built foundational technical knowledge in networking, Linux, scripting, cybersecurity, and cloud through hands-on labs, certifications, and project-based learning while transitioning from a non-technical early role.

EDUCATION

B.S. in Information Technology (Cybersecurity), Western Governors University, Atlanta, GA

2019 — 2023

GPA: 3.8, Dean's List, Relevant Coursework: Network Security, Cloud Computing, Cybersecurity Fundamentals.

M.S. in Cybersecurity, Western Governors University, Atlanta, GA

2023 — 2025

Additional Information

Links: GitHub, Portfolio