

# KEN BRIGHAM

+1 (202) 428-5235 | kenbrigham777@gmail.com | Washington, DC, USA | LinkedIn | GitHub | Portfolio | Website

## CERTIFICATIONS

---

CompTIA - Security+  
CompTIA - Network+  
AWS Certified Cloud Practitioner  
AWS Certified Solutions Architect - Associate  
Google IT Support Professional  
Google Cloud Digital Leader  
Microsoft Azure Fundamentals (AZ-900)

## PROFESSIONAL EXPERIENCE

---

### Cloud Security Internships, Independent Work & Technical Projects

Washington, DC, USA

*Cloud Security & Support Engineer*

*November 2020 - Present*

- Built a home-based SIEM lab using Azure VM, Microsoft Sentinel, and MITRE ATT&CK.
- Developed AWS-native backup automation using EventBridge, Lambda, and EBS ('Smart Vault'). Features scheduled backups, audit logging via DynamoDB, as well as cleanup automation.
- Created 'Silent Scalper', a serverless AWS data pipeline that auto-scales and handles file ingestion with no idle compute.
- Built 'JargonBridge', a generative AI tool that explains cloud security jargon using Claude on AWS PartyRock.
- Completed hands-on threat hunting and log analysis labs via TryHackMe, LetsDefend and HackTheBox.
- Conducted threat analysis and drafted remediation reports during AIG's Shields Up! program.
- Standardized telemetry formats with Python and authored secure dashboard proposals during a virtual internship with Deloitte Australia.
- Tested VPN resilience with Python CLI tools in Verizon's cloud internship; evaluated IAM models during access control simulations for Tata Consultancy Services.

### Various

Washington, DC, USA

*Bartender/Shift Supervisor*

*October 2017 - Present*

- Delivered exceptional service in high-volume settings; built strong interpersonal and multitasking skills.
- Supervised shift operations and trained new staff, maintaining secure payment handling practices.
- Enforced ID verification and alcohol compliance procedures, ensuring guest safety and legal adherence during all shifts.
- Monitored inventory levels and placed supply orders, reducing waste and cutting monthly costs by over 10%.

### 5CA

*IT Support Specialist*

*2019 - 2021*

- Resolved 25+ technical support tickets daily using Zendesk for high-profile gaming clients.
- Utilized VMs, VPNs, and remote desktop tools to troubleshoot user issues across platforms.
- Collaborated with internal teams via Microsoft Teams and Discord to address technical incidents.
- Documented recurring support issues and proposed improvements to internal knowledge base, reducing average resolution time by 15%.
- Delivered technical guidance to non-technical users, translating complex troubleshooting steps into clear, accessible instructions.

## PROJECTS & OUTSIDE EXPERIENCE

---

### 3 Tier Web App

Remote

*DevOps Engineer*

- Designed and deployed a full-stack 3-tier Node.js web application using AWS ECS Fargate, ALB, and RDS PostgreSQL, managed via Terraform.
- Implemented secure infrastructure with SSL-enforced database connectivity, containerized (Docker) backend, and modular IaC for reusability.

### Tata Consultancy Services (TCS) - Cybersecurity Virtual Internship

Remote

*Cybersecurity Analyst Intern*

- Assessed clients' IAM strategy readiness via holistic examinations, and crafted tailored IAM solutions unique to client needs, accounting for organizational structure, existing systems, and current business processes.
- Authored and presented documentation outlining best practice recommendations, utilizing phased implementation strategies with ongoing monitoring & support.

### **Verizon Virtual Internship**

**Remote**

#### *Cloud Platform Engineer*

- Evaluated a cloud-native VPN project for redundancy, resiliency, and security traits using Python CLI tools, then drafted a concise report on the findings.
- Researched and presented security strategies for cloud-based applications across network, data, and application layers.

### **Azure Home-Based SOC**

**Remote**

#### *SOC Analyst*

- The Home-Based SOC project is a functional personal cloud security operations center built on Azure services, featuring log ingestion with Log Analytics, real-time alerting via Azure Monitor, and custom detection rules for tracking suspicious activity across a simulated home network.
- [Link to project](#)

### **AWS Smart Vault**

**Remote**

#### *Cloud Engineer*

- Serverless AWS automation tool - my 'Smart Vault' is used to create, tag, and manage EBS snapshots for EC2 instances based on resource tags.
- It features scheduled backups, audit logging via DynamoDB, and automated cleanup to reduce storage costs.
- [Link to project](#)

### **AWS Silent Scalper**

**Remote**

#### *Cloud Engineer*

- Using event-driven AWS architecture, my 'Silent Scalper' processes incoming files the moment they're uploaded (without pre-provisioned infrastructure), scales automatically, and gracefully handles both success and failure paths.
- Aims to eliminate idle compute waste, as well as file loss resulting from crashes during unpredictable traffic spikes.
- [Link to project](#)

### **Deloitte Australia Job Simulation (Technology)**

**Remote**

#### *Software Engineer*

- Developed a secure dashboard proposal for visualizing IIoT telemetry across four factory sites, incorporating role-based access via internal SSO, restricted intranet-only availability, and structured access to historical machine status logs.
- Developed Python scripts to standardize, validate, and test incoming JSON telemetry data from factory machines, streamlining IIoT data processing and simulation workflows via Repl.it for proposal prototyping.

### **KubeCart - Docker/Kubernetes/EKS/Cloud Run/Flask**

**Remote**

#### *Cloud Engineer*

- KubeCart is a containerized Flask microservice simulating a basic shopping cart API, deployed to AWS using Kubernetes (EKS) and exposed via a public Load Balancer - later migrated to Google Cloud Run.
- Features a live Swagger UI for testing endpoints, built using Flask-RESTX and deployed with Docker, eksctl, and kubectl.

### **AIG Shields Up! Cybersecurity Program**

**Remote**

#### *SOC Analyst Intern*

- Authored and posted an internal advisory regarding a newly discovered zero-day vulnerability affecting Apache Log4j to affected teams.
- Conducted threat analysis and wrote full remediation reports for a ransomware incident; scripted a custom bruteforcer using Python and rockyou.txt to gain access to the maliciously encrypted files.

## **SKILLS**

---

**Skills:** Python, Zendesk, Google Cloud Platform, AWS, Microsoft Azure, SOC, Bash, Confluence, Customer Service, Cryptography, Computer Networking, Docker, Kibana, Kubernetes, Linux/Unix, Microservices, Agile, Terraform, Route 53, Development Operations (DevOps), Splunk, CloudFormation, Git, Wireshark, Atlassian, BigQuery, Elasticsearch, Grafana, Kali Linux, LLM, Machine Learning, MailChimp, MySQL, Nginx, NoSQL, NumPy, PowerShell, Ruby, Ruby on Rails, SQL, Flask, Node.js, Postgres, Postman, REST APIs, Web Development

**Languages:** Spanish, English