JAHIT JANBERK

Cloud Security Engineer | https://jahit.dev | jahitjanberk@proton.me | +447511674137

PROFESSIONAL SUMMARY

Cloud Security Engineer based in London with hands-on experience building serverless AWS architectures, implementing infrastructure as code with Terraform, and operating both defensive (SIEM/XDR) and offensive (penetration testing) security tooling. Currently working at the City of London Police leading national fraud and cybercrime awareness campaigns, with direct exposure to the operational and financial impact of cyber-enabled crime in collaboration with the National Fraud Intelligence Bureau.

EXPERIENCE

Cloud Security Engineer | Independent 2026 – Present

- Design and deploy production AWS environments using S3, CloudFront, Route 53, ACM, Lambda, API Gateway, DynamoDB, IAM, and CloudWatch.
- Implement infrastructure as code with Terraform, deploying full serverless stacks (28+ resources) in a single apply command.
- Enforce least-privilege IAM policies scoped to specific resource ARNs with no wildcard permissions.
- Build secure static-site delivery chains using private S3 origins and Origin Access Control (OAC) policies.
- Develop serverless backend APIs in Python 3.11 with FastAPI, deployed to AWS Lambda behind API Gateway.
- Architect and deliver a cybersecurity incident cost logger (Incident Watch) for SOC analysts, incorporating MITRE ATT&CK tactic tagging and financial impact tracking.
- Delivered marketing and e-commerce sites on AWS for clients including a Cambridge-based synthetic biology startup (Bio Code) and a luxury watch brand (Refuji Watch).

Security Researcher | Homelab2025 – 2026

- Built and operate a dual-track defensive/offensive security homelab spanning physical hardware (2x mini PCs, Raspberry Pi, network switch) and virtualised environments via Proxmox VE.
- Deployed Wazuh as a unified XDR/SIEM platform with agents on all hosts, providing file integrity monitoring, vulnerability detection, and real-time alerting.
- Operated Splunk as a secondary SIEM alongside Wazuh for cross-platform threat hunting and SPL query development.
- Conducted red-team exercises using Kali Linux and Metasploit, generating real attack telemetry ingested by the defensive stack.
- Configured Pi-hole as a network-wide DNS sinkhole to practise DNS-based attack detection and malicious traffic filtering.
- Published a technical homelab walkthrough on DEV Community covering hardware, software choices, and lessons learned.

Digital Designer | City of London Police – Present

- Lead and create national fraud awareness campaigns covering major crime types including courier fraud, investment fraud, ransomware, romance fraud, and social media hacking.
- Collaborated with the Communications Director to develop and launch national public alerts for cybersecurity emergencies.
- Produced digital and print assets for internal and external communications using the Adobe Creative Suite.

- Gained direct operational insight into the financial impact of cyber-enabled fraud, informing the development of Incident Watch — a cost-tracking tool built in collaboration with intelligence from the National Fraud Intelligence Bureau.

PROJECTS

Incident Watch | Serverless SOC Tool · AWS / Python / Terraform2026

- 28 AWS resources defined across 5 Terraform files; full stack deployed and torn down in under 5 minutes via a single terraform apply.
- 4 Lambda functions (one per API route) with pay-per-request DynamoDB billing — £0 server cost at typical SOC team usage volumes.
- Discovered and resolved a Python falsy-validation bug where if not value treated impact: 0 as missing; fixed with explicit None and empty-string checks.

Bio Code | Static Site · AWS / HTML / CSS / JS2026

- Resolved multi-page CloudFront routing by configuring custom error responses — a non-obvious requirement for static sites with more than one HTML file.
- Navigated ACM region constraint (certificates for CloudFront must be requested in us-east-1 regardless of bucket region) without wizard tooling.

Refuji Watch | Brand E-commerce Site · AWS / HTML / CSS / JS2025

- Achieved sub-100ms TTFB from Europe and 100% Lighthouse performance score on desktop with zero EC2 instances.
- Resolved SES sandbox blocking by requesting production access and verifying both sender and recipient addresses before go-live.
- Eliminated stale-content issues by setting short Cache-Control TTLs on HTML files while retaining long TTLs on versioned static assets.

Cybersecurity Homelab | On-Premises Security Lab2025 – Present

- Running Wazuh and Splunk concurrently to compare detection rules and query languages (KQL vs. SPL) against identical attack telemetry.
- Fully on-premises — zero cloud hosting cost; planned expansion to include VLANs, Windows Server/Active Directory, and Ansible/Terraform automation.

CERTIFICATIONS

AWS Certified Cloud Practitioner – Amazon Web Services 2026
Google Cybersecurity Certificate – Google / Coursera 2025
AI Governance Certification – Securiti AI Aug 2025
Google AI Essentials – Google Jul 2025

TECHNICAL SKILLS

AWS (S3, CloudFront, Route 53, ACM, Lambda, API Gateway, DynamoDB, IAM, CloudWatch, SES) · Terraform · Python · JavaScript · HTML/CSS · FastAPI · AWS CLI · Git · Wazuh · Splunk · Kali Linux · Metasploit · Proxmox VE · Pi-hole · MITRE ATT&CK · Adobe Creative Suite