**Professional summary**

Security Engineer with 8+ years of experience designing, implementing, and managing security for AWS, Azure, and GCP environments. Skilled in DevSecOps automation, incident response, cloud-native security posture management, and regulatory compliance. Collaborative servant leader who embeds security early in development lifecycles, mentors teams, and delivers measurable risk reduction.

***Interesting to Know****:* I run a powerful home lab equipped with a comprehensive Security and DevOps toolchain, which enables me to experiment with emerging technologies and hone my skills during weekend CTFs and Red/Blue-team exercises, gaining experience that directly aligns with enterprise offensive and defensive needs.

**Education**

* **Master of Science - Information Technology**   
  *University of the People, Pasadena, CA*
* **Bachelor of Technology – Electrical & Electronics Engineering (Minor: Computer Science)**  
  *University of Buea, Cameroon*

**Certifications**

* CISSP (in Progress) | CISM | CompTIA CASP+ | CompTIA Security+ | AWS Security - Specialty | AWS Cloud Practitioner | Microsoft Cybersecurity Architect - Expert | Azure Security Engineer - Associate| Certified Scrum Product Owner

**Technical Skills**

* **Cloud & DevSecOps:** AWS, Azure, GCP, Oracle Cloud | Terraform, CloudFormation, Ansible, ARM
* **Identity & Access Management:** AWS/GCP IAM, Azure AD, Okta, SSO, MFA, RBAC/ABAC, PAM
* **Security Operations & Monitoring:** Splunk, Azure Sentinel, Chronicle, Phantom SOAR | CrowdStrike Falcon (EDR & CSPM), Tenable, Jira/Confluence.
* **Application Development / Security:** Visual Studio Code, Git | REST/SOAP API Design & Security | HTML, XML, JavaScript, Java, Golang | Veracode (SAST/DAST/SCA), OWASP Top 10 | ZAP, Snyk | Secure SDLC, Shift-Left Security, JIRA Integration, Burp Suite,
* **Networking & Infrastructure:** Zero Trust, VPC/VNET Segmentation, VPN | Firewalls (Palo Alto, Cisco, Forticlient), WAF, DDoS
* **Compliance & Governance:** NIST, ISO 27001/2, CIS, PCI-DSS, HIPAA, GDPR, SOC 2
* **Scripting & Automation:** Python (Boto3), Bash, PowerShell | CI/CD (Jenkins, GitHub Actions, GitLab CI), Kubernetes (EKS, AKS), Helm

**Professional experience**

**CVS Healthcare | Woonsocket, RI**  
***Role: Lead Engineer – Product & Cloud Security*** | Apr 2022 – Present

* Developed an **AWS security-automation framework** with **Terraform** & **Python**, which cut manual effort by 40 %, so analysts refocused on threat hunting.
* Redesigned **incident response** using **CrowdStrike Falcon SOAR** playbooks, which enabled **auto-remediation**, so **MTTR** fell 35 %.
* Rebuilt **shift-left security** into **CI/CD pipeline** in **GitHub Actions** with **Veracode**, which gave developers instant feedback, so 20 % more **vulnerabilities** were blocked pre-merge.
* Reviewed and unified logs from **Splunk SIEM**, **CrowdStrike EDR**, and **Tenable**, which **streamlined investigations**, so alert fatigue dropped 35 %.
* Developed **policy-as-code** gates using **Checkov** and**OPA,** which stopped non-compliant Terraform deployments at **PR time**, resulting in production misconfigurations falling to near zero.
* Rebuilt **auto-ticketing** by linking **Tenable, CrowdStrike, and GitHub** findings to **Jira**, which enforced ownership, so **high/critical issues** hit 100 % closure.
* Reviewed AWS posture through continuous **Zero-Trust audits** of **KMS**, **IAM Roles**, **VPC**, **ALB/WAF**, and **SCPs**, which removed 50+ risky permissions, so access risk shrank sharply.
* Developed **CrowdStrike CSPM** for 50+ AWS accounts with **auto-remediation Lambdas**, which fixed **Indicators of** **Misconfigurations** in real time, so 10+ issues were closed weekly.
* Redesigned **threat modeling** for **Lambda**, **EKS**, and **Fargate** migrations, which surfaced 12 critical issues pre-prod, so launches went live with zero blockers.
* Rebuilt the **EKS** security baseline using Terraform & **OPA Gatekeeper**, which enforced **pod/network policies**, so privileged containers were fully blocked.
* Developed **secrets governance** with **Vault** and **AWS Secrets Manager**, which eliminated hard-coded credentials, so secret-leak findings dropped to zero.
* Reviewed **post-incident reports** and briefed the **CISO** weekly, which linked progress to the **NIST CSF**, so budget for next-quarter initiatives was approved.
* Redesigned **knowledge-sharing** via bi-weekly **DevSecOps workshops**, which spread AWS best practices, so 90 % of repos now pass secure-pipeline gates.
* Collaborated with the Compliance team to **review security controls** for **3 compliance audits** **(HIPAA, SOC 2 Type 1, HIPAA, PCI-DSS, HiTrust, HiTECH)**, which kept controls in continuous readiness, so pass rates stayed above 95 % and regulated-market revenue remained protected.

**Morgan Stanley | New York, NY**  
***Role:******Lead Engineer – Corporate Infrastructure and Security*** | Feb 2019 – Mar 2022

* Oversaw a **rapid migration** from on-prem to **Azure**, which delivered hardened **IAM**, **SSO/MFA**, and **PAM**, so identity-threat alerts fell 45 % while 10k+ employees pivoted to remote work during the **COVID period**.
* Rebuilt **remote-access architecture** with **Azure AD Conditional Access**, **VPN Gateway**, and **risk-based MFA**, which stabilized home-office logins, so access-related tickets dropped 60 % and uptime stayed 99.9 %.
* Reviewed and **automated patch/compliance** via **Ansible** and **PowerShell**, which removed manual interventions, so ops effort plummeted 50% despite reduced on-site staff.
* Redesigned **AKS** **security baselines** using **Azure Policy** and **Defender for Kubernetes**, which enforced **CIS controls**, so clusters reached 99 % compliance.
* Developed a **secure AKS pipeline** in **Azure DevOps** / **GitHub Actions** with **Trivy** scans and **Kyverno** policies, which blocked non-compliant **images**, so only hardened workloads hit production.
* Reviewed the **SDLC** to embed **Snyk** and **OWASP ZAP** scans, which met **SOC 2 Type 1** and **ISO 27001** controls, so secure releases shipped 30% faster.
* Rebuilt **API security** using **Azure API Gateway** and custom **Java rate-limiting**, which throttled abuse attempts, so **REST API** incidents fell sharply.
* Developed a **Zero-Trust** framework on **Azure AD (Entra ID)**, which constrained lateral movement, so privileged-access incidents dropped to zero.
* Redesigned **security awareness** for remote staff through weekly micro-trainings and **phishing drills**, which boosted safe-WFH hygiene, so click-through on phishing tests fell from 22 % to 5 %.
* Reviewed **business-continuity playbooks** under COVID pressure, which aligned IT, SecOps, and HR, so all migrations finished two months ahead of the deadline without downtime.

**Cameroon Telecommunication (CAMTEL) | Douala, Cameroon**  
***Role: Infrastructure Security Engineer*** | Dec 2016 – Jan 2019

* Promoted from Junior Security Engineer to Level II Infrastructure Security Engineer.
* Reviewed and implemented **GCP hardening** for VPC service controls and IAM least privilege.
* Deployed **SIEM, EDR, and CASB** tools, improving **incident response** efficiency by 30%.
* Optimized **firewalls/WAFs** to boost resilience by 25% and ensure national regulatory compliance.