Cloud Security Architect – 4-Month Internship-Style Course

Student: Olakunle Paul Omoniyi
Instructor: Professor of Cloud Security (AI Tutor)
Format: 16 Weeks | Daily Labs | MIT/Harvard-Style

Program Learning Goals

- Master Linux & Python for cloud security automation
- Deploy and secure workloads on AWS, Azure, and GCP
- Design & defend with SIEM (Splunk, Sentinel, Chronicle)
- Perform red-team hacking techniques (ethical) and blue-team defense
- Build a job-ready GitHub portfolio with labs, scripts, and architecture docs
- Graduate with a binder-ready syllabus + HR-friendly repo

Month 1 – Foundations

Week 1: Linux for Security – CLI, processes, logging, hardening, auditd, log shipping
Week 2: Python for Security – log parsing, AWS/Azure/GCP SDKs, detections, packaging
Week 3: AWS Security Essentials – IAM, CloudTrail, GuardDuty
Week 4: Azure Security Basics – Azure AD, RBAC, Defender, Sentinel

Month 2 – Multi-Cloud Security

Week 5: GCP Security 101 – IAM, VPC SC, Chronicle
Week 6: SIEM Mastery – Splunk, ELK, Azure Sentinel
Week 7: Network Security – Firewalls, WAF, VPN, Zero Trust
Week 8: Hacking Techniques – Recon, phishing, exploitation

Month 3 – Defense & Automation

Week 9: Incident Response in Cloud – playbooks, automation, SOAR
Week 10: Zero Trust Architecture – SCPs, Conditional Access, BeyondCorp
Week 11: Python + Cloud Security Automation – Boto3, Azure SDK, GCP API
Week 12: Cloud Forensics – memory capture, log analysis, timelines

Month 4 – Advanced & Career Prep

Week 13: AI in Cloud Security – anomaly detection with ML
Week 14: Capstone Project – Red vs Blue simulation
Week 15: Resume + GitHub Showcase – convert labs into portfolio projects
Week 16: Final HR-Friendly Presentation – architecture diagrams + design