A TWELVE MONTH PATH

Learn cloud security. *Then prove it.*

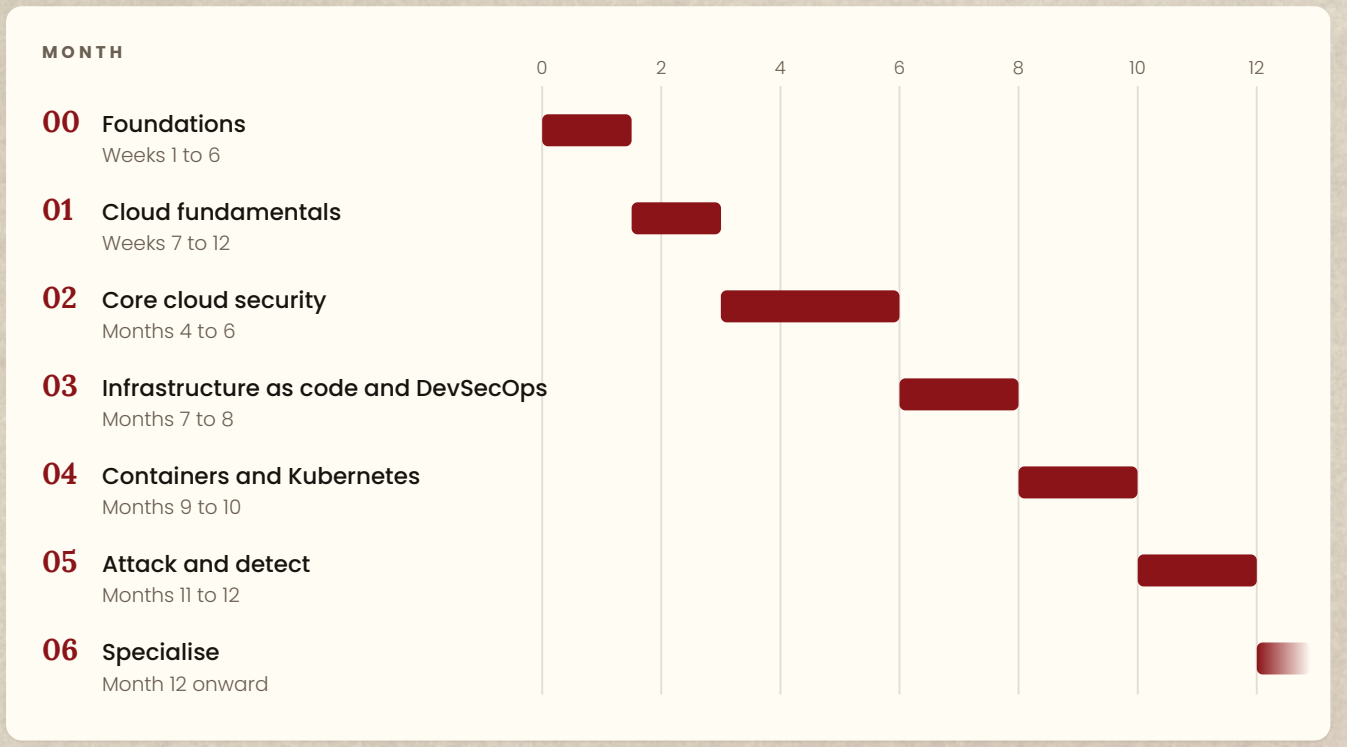
From zero to job ready in seven phases. One cloud first, free tools first, and a portfolio that does the talking for you.

About 10 hours a week | 7 phases | 6 portfolio projects | Certificates optional

MICHAEL ADEYANJU
michaeladeyanju.com

Twelve months.
Seven phases. One cloud.

Each phase has four parts. **Learn** is the theory. **Practice** is a free lab. **Prove it** is a project you put on GitHub. **Checkpoint** tells you when you are ready to move on.



FIVE RULES BEFORE YOU START

- **Pick one cloud.** AWS is the safe default: the most job posts and the most free labs. Choose Azure if your local market runs on Microsoft. Add a second cloud in Phase 06, not before.
- **Build, break, fix.** Reading about a misconfiguration teaches you less than making one and cleaning it up.
- **Protect your wallet.** Set a billing alarm before you create anything. Tear down every lab when you finish.
- **Never put real keys in code.** Automated scanners watch public repositories for credentials all day.
- **Write as you learn.** One short post per phase. That is your portfolio and your network, built at the same time.

MICHAEL ADEYANJU
michaeladeyanju.com

00

Weeks 1 to 6

Foundations first.
The cloud comes later.

Cloud security is networking, Linux and identity with an API in front. Skip this phase and every later one gets harder.

LEARN

- **Networking.** TCP/IP, ports, DNS, HTTP and TLS, subnets and CIDR, NAT, routing.
- **Linux.** Permissions, processes, services, SSH, logs, package managers.
- **Scripting.** Python for automation, Bash for glue, reading JSON and YAML without fear.
- **Security basics.** Authentication versus authorisation, hashing versus encryption, least privilege, the CIA triad.
- **Git.** Commits, branches, pull requests. Everything you build from here lives in a repository.

PRACTICE

OverTheWire Bandit

TryHackMe Pre Security

Python for Everybody

Linux Journey

PROVE IT

Write a Python script that reads an SSH auth log and flags repeated failed logins by IP. Push it to GitHub with a clear README.

CERTIFICATE, OPTIONAL

CompTIA Security+. Useful for getting past HR filters on entry roles. Not required to learn anything here.

CHECKPOINT: YOU ARE READY WHEN

You can explain what happens when you type a URL and press enter, from the DNS lookup to the TLS handshake to the response.

COMMON TRAP Rushing this phase because it feels basic. Almost every cloud misconfiguration you will ever fix is a networking or identity mistake underneath.

MICHAEL ADEYANJU
michaeladeyanju.com

01

Weeks 7 to 12

Learn one cloud. *Learn it properly.*

You cannot secure what you cannot build. Spend this phase building, not watching videos.

LEARN

- **Shared responsibility.** What the provider secures, and what is always yours.
- **The layout.** Accounts, regions, availability zones.
- **Identity.** Users, groups, roles and policies. This is the most important service you will learn.
- **Core services.** EC2 and Lambda for compute, S3 and EBS for storage, RDS and DynamoDB for data.
- **Networking.** VPCs, subnets, route tables, internet and NAT gateways, security groups.
- **Billing.** Budgets, alarms and free tier limits. Learn these on day one.

PRACTICE

AWS Skill Builder · AWS Free Tier · Microsoft Learn (Azure) · AWS CLI

PROVE IT

Host a static website on S3 behind CloudFront. Bucket private, HTTPS only. Then tear it down and rebuild it using only the CLI.

CERTIFICATE, OPTIONAL

AWS Solutions Architect Associate is the stronger signal. Cloud Practitioner only if you are new to tech. Azure route: AZ-900, then AZ-104.

CHECKPOINT: YOU ARE READY WHEN

You can draw a VPC with public and private subnets from memory and say which traffic can flow where, and why.

COMMON TRAP Collecting services. Ten services understood deeply beat fifty you clicked through once.

MICHAEL ADEYANJU
michaeladeyanju.com

02

Months 4 to 6

Core cloud security. *Where the job lives.*

Most cloud breaches are not clever. They are a public bucket, a leaked key, or a role that can do far too much. **This phase is about exactly those.**

LEARN

- **Identity.** Least privilege, roles over long lived keys, MFA, permission boundaries, SCPs, SSO and federation, IAM Access Analyzer.
- **Network.** Security groups versus NACLs, private subnets, VPC endpoints, WAF, egress control.
- **Data.** KMS and key policies, encryption at rest and in transit, Secrets Manager, S3 Block Public Access.
- **Logging and detection.** An organisation wide CloudTrail, VPC Flow Logs, GuardDuty, Security Hub, Config rules.
- **Governance.** Multi account setups with AWS Organizations, CIS Benchmarks, the Well-Architected Security Pillar.
- **Posture tools.** Prowler and ScoutSuite, run against your own account.

PRACTICE

AWS Workshops · Prowler · CIS Benchmarks · IAM Policy Simulator

PROVE IT

Run Prowler against your lab account. Fix the top ten findings. Publish a before and after write up that explains each fix in plain words.

CERTIFICATE, OPTIONAL

AWS Certified Security Specialty. Azure: AZ-500. Google Cloud: Professional Cloud Security Engineer. This is the core cert of the whole roadmap.

CHECKPOINT: YOU ARE READY WHEN

Given any IAM policy, you can say exactly what it allows, what it should not allow, and how you would tighten it.

COMMON TRAP Treating the tool as the job. Prowler lists hundreds of findings. Your value is knowing which three matter this week.

MICHAEL ADEYANJU
michaeladeyanju.com

03

Months 7 to 8

Clicking does not scale. *Code does.*

Real teams build cloud with code. Security that lives in the pipeline catches the mistake before it ships, not after it leaks.

LEARN

- **Terraform.** Providers, state, modules. Remote state holds secrets, so lock it down.
- **CI/CD.** GitHub Actions, and OIDC federation to the cloud instead of stored access keys.
- **IaC scanning.** Checkov and Trivy against every pull request.
- **Secret scanning.** gitleaks in a pre-commit hook and in the pipeline.
- **Policy as code.** Open Policy Agent and Conftest to turn rules into tests.
- **Supply chain.** Dependency scanning, pinned actions, SBOMs.

PRACTICE

TerraGoat · Checkov · Trivy · gitleaks · GitHub Actions

PROVE IT

Rebuild your Phase 02 environment in Terraform. Add a pipeline that fails the build on a public bucket, an open security group or a hardcoded secret.

CERTIFICATE, OPTIONAL

HashiCorp Terraform Associate. Worth it for DevSecOps and platform roles.

CHECKPOINT: YOU ARE READY WHEN

Nothing in your lab is created by hand any more, and a bad change cannot reach your account without a red build.

COMMON TRAP Committing Terraform state to Git. State files can hold secrets in plain text.

MICHAEL ADEYANJU
michaeladeyanju.com

04

Months 9 to 10

Containers are processes. *Kubernetes is an API.*

Most modern workloads run in containers. Kubernetes adds a powerful API, and every powerful API is an attack surface.

LEARN

- **Docker.** Images and layers, minimal base images, non-root users, read only filesystems.
- **Image security.** Scanning with Trivy or Grype, signing with cosign, private registries.
- **Kubernetes.** Pods, deployments, services, namespaces.
- **Kubernetes security.** RBAC, network policies, Pod Security Admission, secrets, service account tokens.
- **Managed clusters.** EKS, AKS or GKE, and how pods get cloud permissions (IRSA, EKS Pod Identity).
- **Runtime.** Falco for detecting what a container does after it starts.

PRACTICE

Kubernetes Goat · kind or minikube · kube-bench · EKS Cluster Games

PROVE IT

Deploy an app to a local cluster, then lock it down: non-root, read only filesystem, network policy, least privilege RBAC. Show kube-bench results before and after.

CERTIFICATE, OPTIONAL

CKA first, then CKS, which needs a CKA pass. Hands on exams, so they carry real weight with container heavy teams.

CHECKPOINT: YOU ARE READY WHEN

You can explain how a compromised pod could reach the cloud account behind it, and the three controls that stop it.

COMMON TRAP Running everything as root because the tutorial did. Most tutorials optimise for working, not for safe.

MICHAEL ADEYANJU
michaeladeyanju.com

05

Months 11 to 12

Think like the attacker. *Then catch them.*

Defenders who have attacked a cloud account write better detections. Do both, in labs you own.

LEARN

- **Attack paths.** Leaked keys, SSRF to instance metadata (IMDSv1 versus v2), IAM privilege escalation, public snapshots.
- **Frameworks.** The MITRE ATT&CK Cloud matrix as your map of techniques.
- **Offensive tools.** Pacu and CloudFox for enumeration and escalation.
- **Detection engineering.** Alerts written from CloudTrail, Sigma rules, attacks simulated with Stratus Red Team.
- **Incident response.** Isolate, snapshot, preserve logs, rotate credentials, write it up.

PRACTICE

flaws.cloud · flaws2.cloud · CloudGoat · The Big IAM Challenge · Hacking the Cloud

PROVE IT

Run a Stratus Red Team technique in your lab. Catch it with a detection you wrote. Then write the incident report as if a manager will read it.

CERTIFICATE, OPTIONAL

No cert needed here. Your write ups are the credential.

CHECKPOINT: YOU ARE READY WHEN

Given a leaked access key, you can name the first five things an attacker does, and the first five things you do.

COMMON TRAP Testing targets you do not own. Only test accounts you own or have written permission to test, and read the provider testing policy first.

MICHAEL ADEYANJU
michaeladeyanju.com

06

Month 12 onward

Go deep. *Then go wide.*

Twelve months makes you job ready. A specialty is what gets you picked over the next candidate. Choose one track, and add a second cloud. Azure is the usual pick, because Entra ID is a world of its own.

PICK ONE TRACK

Cloud security engineering

Landing zones, guardrails, multi account design. The path to architect.

DevSecOps and platform

Supply chain security, SLSA, policy as code across hundreds of repos.

Cloud penetration testing

Deeper offensive labs, then real engagements under a signed scope.

Detection and response

SIEM, threat hunting in cloud logs, response runbooks.

AI workload security

Securing LLM apps and model pipelines. Start with the OWASP Top 10 for LLM Applications.

Governance and compliance

ISO 27001, SOC 2, and data protection law such as the NDPA in Nigeria or GDPR in Europe.

CERTIFICATES FOR THIS STAGE

CCSK for vendor neutral breadth. CCSP once you have the required years of experience. A second cloud's security cert when you add that cloud.

MICHAEL ADEYANJU
michaeladeyanju.com

A cert gets you past the filter. *A project gets you the job.*

Certificates are optional on this roadmap. Take one when a job post you want asks for it, or when an exam deadline would help you finish a phase. Never take one instead of building.

PHASE	CERTIFICATE	WORTH IT FOR
00	CompTIA Security+	Entry roles and HR filters
01	AWS Solutions Architect Associate / AZ-104	Shows you can build, not just describe
02	AWS Security Specialty / AZ-500 / Google PCSE	The core cloud security credential
03	HashiCorp Terraform Associate	DevSecOps and platform roles
04	CKA, then CKS	Container heavy teams; hands on exams
06	CCSK (Cloud Security Alliance)	Vendor neutral breadth
06	CCSP (ISC2)	Senior and architect roles; experience required

IF BUDGET IS TIGHT

Skip the foundational exams. Put the money toward one associate level build cert and the security specialty. Spend the rest of the time on projects, which cost nothing.

Six projects. One GitHub. *That is your CV.*

Every phase ends in something you can show. Give each project a README that says what you built, what was insecure, what you changed, and how you proved it.

YOUR PORTFOLIO

00 SSH log analyser in Python

01 Private S3 website behind CloudFront, rebuilt by CLI

02 Prowler before and after write up

03 Terraform environment with a security pipeline

04 Hardened Kubernetes deployment with kube-bench evidence

05 Detection plus incident report from a simulated attack

Bonus. One blog post per project. Recruiters read posts. Hiring managers read READMEs.

FREE RESOURCES

LEARN

- AWS Skill Builder
- Microsoft Learn
- Google Cloud Skills Boost
- Well-Architected Security Pillar
- CIS Benchmarks
- Hacking the Cloud

LABS

- flaws.cloud
- flaws2.cloud
- CloudGoat
- TerraGoat
- Kubernetes Goat
- The Big IAM Challenge
- EKS Cluster Games
- Pwned Labs

TOOLS

- Prowler
- ScoutSuite
- Pacu
- CloudFox
- Trivy
- Checkov
- Falco
- Stratus Red Team

WATCH AND READ

- fwd:cloudsec talks
- Practical Cloud Security, Chris Dotson
- Hacking Kubernetes, Martin and Hausenblas

MICHAEL ADEYANJU
michaeladeyanju.com

Where the roadmap *can take you.*

ROLE	KEY PHASES	WHAT YOU DO
Cloud Security Engineer	02, 03, 05	Secures accounts, identity and pipelines day to day.
DevSecOps Engineer	03, 04	Puts security into the build and deploy process.
Cloud Penetration Tester	02, 05	Attacks cloud estates under a signed scope.
Detection Engineer	02, 05	Turns cloud logs into alerts that matter.
Cloud GRC Analyst	02, 06	Maps controls to standards and evidence.
Cloud Security Architect	All, plus years	Designs the guardrails everyone else works inside.

Nobody hires a roadmap. *They hire what you built while following it.*

Questions, a portfolio review, or mentoring on any phase: find me at michaeladeyanju.com.

MA

MICHAEL ADEYANJU
michaeladeyanju.com