

 **INDUSTRY READY CERTIFICATION PROGRAM**

Cloud Security Engineer Program

Master **AWS, Azure and GCP security**, cloud pentesting and DevSecOps with live labs, real projects and an internship. Built to take you from beginner to a job ready Cloud Security Engineer.

12
WEEKS

3 Days
PER WEEK

Live
+ RECORDINGS

5+
REAL PROJECTS

Fri, Sat & Sun
8:00 to 9:30 PM IST

02 THE OPPORTUNITY

Why Cloud Security?

Every company is moving to the cloud, and almost none have enough people to secure it. Cloud security is one of the **highest paid and fastest growing** skills in tech today.

3.5M

Unfilled cybersecurity jobs worldwide

115%

Growth in cloud security roles since 2022

#1

Most in demand cloud skill for 2026



Strong Salary Range

Cloud security engineers in India earn 8 to 30 LPA, and senior roles go well beyond, with global remote roles paying even more.



Recession Resistant

Security is the last budget companies cut. Cloud adoption keeps rising, and so does the need to protect it.



Every Industry Hiring

Banking, healthcare, SaaS, e-commerce and government all need cloud security talent right now.



Fast Career Growth

Move from analyst to engineer to architect quickly. Skills here compound faster than most IT tracks.

03 PROGRAM OVERVIEW

A Complete Job Ready Program

Learn live, practice in real labs, build projects and walk out with a certification and internship experience.

12 Weeks

TOTAL DURATION

Fri · Sat · Sun

3 DAYS EVERY WEEK

**8:00 – 9:30
PM**

IST · LIVE CLASS



Live + Recordings

Attend live and keep lifetime access to every class recording.



Internship

An internship to apply your skills on real cloud workloads.



Certification

Techonquer Certified Cloud Security Engineer on completion.



Real Projects

5+ portfolio grade projects that prove your skills to recruiters.

04

AUDIENCE

Who Should Join?

This program is built for anyone who wants to break into or level up in cloud and security, whether you are just starting or already working in tech.



Students & Final Year Learners

Get a head start with job ready cloud security skills before you graduate.



Freshers

Enter cybersecurity through one of its highest paying and most in demand doors.



DevOps Engineers

Add security to your pipeline skills and grow into a DevSecOps role.



Security Engineers

Specialize in cloud and multiply your value across AWS, Azure and GCP.



Career Switchers

Move from IT, networking or support into a future proof cloud security career.

05 CAREER ROADMAP

Your Path To Cloud Security Engineer

A clear, step by step journey. Each stage builds on the last so you are never lost and always moving forward.



START HERE

Student / Fresher

Begin with zero assumptions. No prior cloud experience needed.



STAGE 1

Cloud Fundamentals

Core AWS, Azure and GCP services, networking and IAM basics.



STAGE 2

Cloud Security

Identity, data protection, monitoring and threat detection.



STAGE 3

DevSecOps

Secure CI/CD, IaC scanning and automation across pipelines.



OUTCOME

Cloud Security Engineer

Job ready, certified and backed by real projects.

06 TOOLS & TECHNOLOGIES

Tools You Will Master

Train on the exact platforms and tools used by cloud security teams in production, across cloud providers, containers, automation and scanning.

CLOUD PLATFORMS

 **AWS**
 **Microsoft Azure**
 **Google Cloud**

CONTAINERS & ORCHESTRATION

 **Docker**
 **Kubernetes**

AUTOMATION & CI/CD

 **Terraform**
 **Jenkins**
 **GitHub Actions**

CLOUD SECURITY & SCANNING

 **Trivy**
 **Prowler**
 **Wiz**
 **Prisma Cloud**

07 LEARNING PATH

Level 1: Beginner

BEGINNER

Weeks 1 to 3 | Foundations


Cloud Computing Basics

IaaS, PaaS, SaaS, regions, availability zones and shared responsibility.


Core Compute & Storage

EC2, S3, VMs, blob storage and managed databases explained simply.


Cloud Networking

VPC, subnets, security groups, routing and load balancing.


IAM Fundamentals

Users, roles, policies and the principle of least privilege.


CLI & Console

Work confidently with AWS CLI, Azure CLI and gcloud.


Linux & Scripting

The command line and scripting skills every engineer needs.

08 LEARNING PATH

Level 2: Intermediate

INTERMEDIATE

Weeks 4 to 6 | Securing the Cloud


Identity Security

Advanced IAM, federation, MFA and conditional access.


Data Protection

Encryption at rest and in transit, KMS and secrets management.


Logging & Monitoring

CloudTrail, CloudWatch, Azure Monitor and GCP logging.


Threat Detection

GuardDuty, Defender for Cloud and Security Command Center.


Network Security

Firewalls, WAF, private endpoints and segmentation.


Compliance Basics

CIS benchmarks, well architected and security baselines.

09 LEARNING PATH

Level 3: Advanced

ADVANCED

Weeks 7 to 9 | Offense & Automation


Cloud Pentesting

SSRF to metadata, IAM abuse and privilege escalation paths.


S3 & Storage Attacks

Enumeration, misconfiguration and data exposure testing.


DevSecOps Pipelines

Shift left security with scanning built into CI/CD.


Infrastructure as Code

Terraform security, drift detection and policy as code.


Container Security

Image scanning, runtime security and Kubernetes hardening.


Attack Path Analysis

Map and break real attacker paths across cloud accounts.

10 LEARNING PATH

Level 4: Expert

EXPERT

Weeks 10 to 12 | Architect & Respond


Secure Architecture

Design enterprise grade, multi account secure cloud setups.


Threat Hunting

Proactively hunt threats across cloud logs and telemetry.


Incident Response

Detect, contain and recover from real cloud incidents.


Capstone Project

Build and defend a full enterprise cloud environment.


Interview Prep

Mock interviews, resume and portfolio review.


Job Readiness

Certification, internship and placement support.

11 OFFENSIVE SECURITY

Cloud Pentesting

Think like an attacker. Learn the real techniques used to break into cloud environments, so you can find and fix them first.



SSRF to Metadata

Abuse server side request forgery to reach the instance metadata service and steal cloud credentials.

CREDENTIAL THEFT



IAM Abuse

Exploit over permissive roles and policies to escalate from low access to full account control.

PRIVILEGE ESCALATION



S3 Enumeration

Discover and test misconfigured storage buckets that leak sensitive company data.

DATA EXPOSURE



Attack Path Analysis

Chain misconfigurations across accounts to map how a real breach would unfold.

LATERAL MOVEMENT

12 DEVSECOPS

Security Built Into Every Pipeline

Shift security left. Learn to automate scanning, secrets detection and compliance directly inside the development workflow.



Terraform

Write secure infrastructure as code, scan it for misconfigurations and enforce policy as code before anything is deployed.



GitHub Actions

Automate security checks on every commit and pull request with hardened, least privilege workflows.



Jenkins

Build secure CI pipelines with integrated SAST, dependency and container image scanning.



Secure CI/CD

Design end to end pipelines where security gates block risky code from ever reaching production.

13 HANDS ON PROJECTS

Build Real Projects

Theory does not get you hired, proof does. Every project here is portfolio grade and built to show recruiters you can do the job.



PROJECT 01

Secure VPC Deployment

Design and deploy a hardened, segmented cloud network with private subnets and strict controls.



PROJECT 02

Enterprise Architecture

Architect a secure multi account cloud setup following well architected best practices.



PROJECT 03

Threat Hunting

Hunt for malicious activity across cloud logs and build detection rules.



PROJECT 04

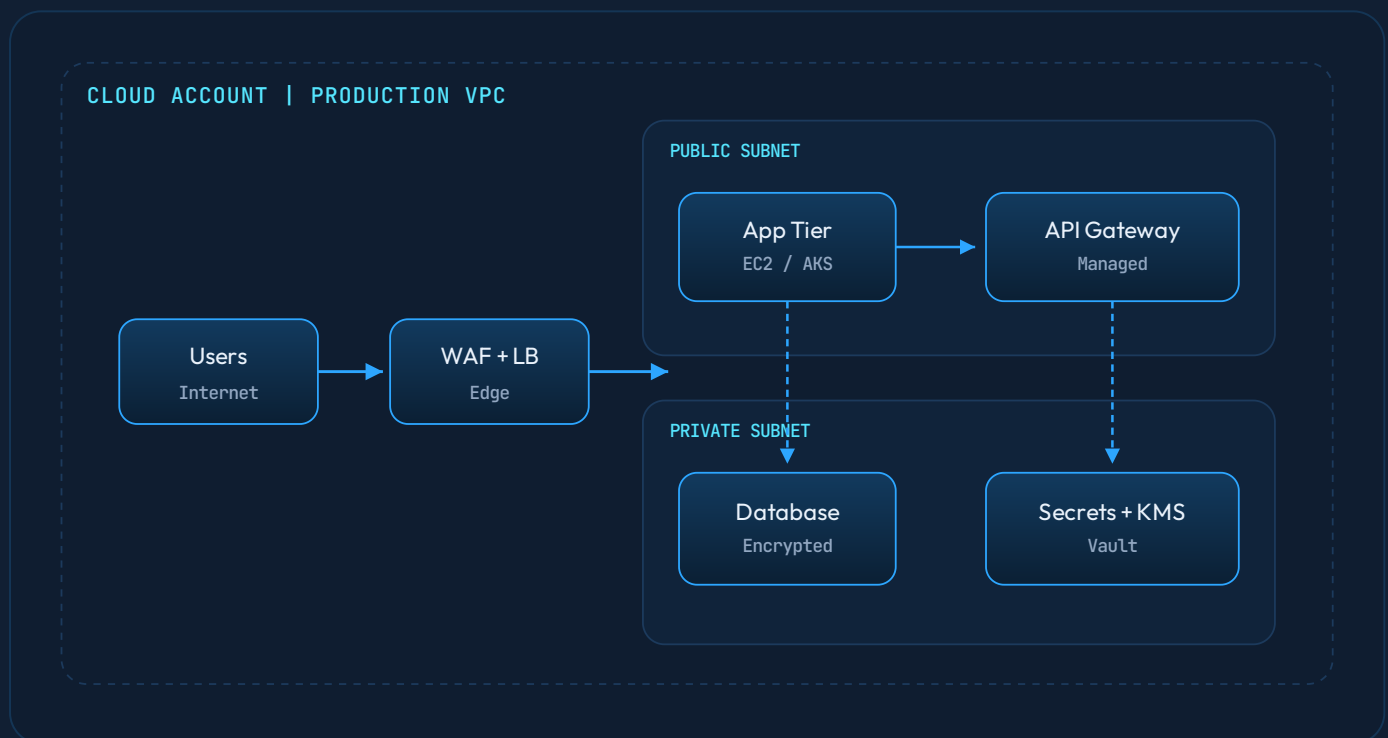
Incident Response

Run a full IR cycle on a simulated cloud breach from detection to recovery.

14 CAPSTONE

Capstone: Secure Enterprise Cloud

Bring everything together. Design, deploy, secure and defend a complete enterprise cloud architecture, exactly like the real diagrams you will own on the job.



✓ Segmented VPC

✓ Least Privilege IAM

✓ Encryption + KMS

✓ Monitoring + Alerts

15 CERTIFICATION

Get Certified

Finish the program and earn a credential that proves your skills to employers across India and beyond.



CERTIFICATE OF COMPLETION

Techonquer Certified Cloud Security Engineer

Awarded to learners who complete all modules, labs, projects and the capstone. Shareable on LinkedIn and verifiable by employers.

✓ Industry Recognized

✓ LinkedIn Shareable

✓ Verifiable

16 CAREER OPPORTUNITIES

Roles You Can Land

This program opens the door to multiple high paying cloud and security roles. Indicative annual salary ranges in India are shown below.

	Cloud Security Analyst		6 - 12 LPA
	Cloud Engineer		8 - 16 LPA
	DevSecOps Engineer		12 - 24 LPA
	Cloud Pentester		12 - 26 LPA
	Security Consultant		15 - 30 LPA

Ranges are indicative and vary with experience, location and company. Senior and remote roles often pay significantly more.

17 WHY TECHONQUER

Why Learn With Technoquer?

We do not just teach theory. We build engineers with real, demonstrable skills and the support to actually get hired.



Live Hands On Labs

Practice every concept in real cloud environments, not slides. Learn by breaking and fixing.



Industry Mentors

Learn from practitioners who secure real cloud workloads every day.



Internship Included

Apply your skills on real projects and add genuine experience to your resume.



Real Projects

Graduate with a portfolio that proves to recruiters you can do the work.



Career & Placement Support

Resume reviews, mock interviews and job referrals to help you land the role.



Start Your **Cloud Security** Career

Seats are limited for each live cohort. Enroll now and get the full curriculum, labs, internship and certification.



EMAIL

team@technoquer.org



CALL / WHATSAPP

+91 63670 98233



WEBSITE

technoquer.org



ENROLL / DEMO

courses.technoquer.org

Enroll Now

 **aws**

 **Azure**

 **Google Cloud**