

Cloud Security Engineering

Secure cloud identities, networks, data, workloads and delivery pipelines - then investigate and respond to cloud attacks.

**8 weeks**

DURATION

78 hours

GUIDED LEARNING

2 projects

PORTFOLIO



ABOUT THE ACADEMY

Practical learning. Work you can demonstrate.

Brightnest AI Academy brings live instruction, guided practice and career preparation together for individuals and teams.

23

FOCUSED COURSES

6

FLAGSHIP PROGRAMMES

Noida

ACADEMY LOCATION

Our approach

1

Learn

Understand concepts through live instruction and current examples.

2

Build

Apply learning through labs, assignments and guided projects.

3

Explain

Document decisions, results, trade-offs and limitations.

4

Prepare

Connect completed work with CVs, interviews and workplace conversations.

PEOPLE BEHIND THE ACADEMY

Meet Ranjeet Kumar



ACADEMY ADVISER

Ranjeet Kumar

Innovation & Growth Leader

15+ years

Experience in data, artificial intelligence and machine learning leadership.

Areas of expertise

- Data science and machine learning solution leadership
- AI product strategy and scalable data platforms
- Technology team leadership and mentorship
- Practical AI and data adoption for business transformation

Education

Master of Information Systems, Anna University, Chennai
Bachelor of Computer Science Engineering



COURSE OVERVIEW

Build your next set of skills

Secure cloud workloads, identities, networks, data and DevSecOps pipelines. Progress from Cloud Security Architecture and Shared Responsibility to Governance, Compliance and Cloud Security Capstone through guided labs, assessed projects, and portfolio evidence.

Who this is for

Cloud, security and DevOps professionals specialising in cloud-security engineering.

Before you begin

Learners should understand cloud and cybersecurity fundamentals. Prior exposure to AWS, Azure, or Google Cloud is helpful.

Cloud security requires coordinated controls across identity, networks, workloads, data, pipelines, posture management, and incident investigation.



LEARNING OUTCOMES

What you will be able to do

01

Threat-model a cloud application and identify responsibility/control ownership.

02

Redesign an overprivileged cloud IAM model and implement least-privilege roles in a lab.

03

Design secure network segmentation for a three-tier cloud workload.

04

Implement a secrets and encryption strategy for application/data services.

05

Assess a containerised workload and design preventive/detective controls.

06

Investigate a simulated cloud account compromise and execute a response playbook.

07

Secure an end-to-end cloud application and present architecture, controls, detections and incident plan.



CURRICULUM

Course curriculum

8 modules · 8 weeks · 78 hours of guided learning

01 Cloud Security Architecture and Shared Responsibility

6 hours

TOPICS

Cloud service models · Shared responsibility · Threat modeling · Landing zones · Multi-account/subscription/project strategy · Zero trust principles

PRACTICAL WORK

Threat-model a cloud application and identify responsibility/control ownership.

Tools: Cloud architecture tools

Assessment: Architecture case

Portfolio evidence: Cloud threat model

02 Cloud IAM and Privileged Access

10 hours

TOPICS

Cloud identities · Roles/policies · Least privilege · Workload identities · Federation · MFA · Privileged access · Service accounts · Keyless patterns

PRACTICAL WORK

Redesign an overprivileged cloud IAM model and implement least-privilege roles in a lab.

Tools: AWS/Azure/GCP IAM concepts

Assessment: IAM lab

Portfolio evidence: Cloud IAM control matrix

CURRICULUM

Course curriculum

8 modules · 8 weeks · 78 hours of guided learning

03 Network and Perimeter Security

8 hours

TOPICS

VPC/VNet design · Segmentation · Private endpoints · Security groups/NSGs/firewalls · WAF · DDoS concepts · Egress controls · Service-to-service security

PRACTICAL WORK

Design secure network segmentation for a three-tier cloud workload.

Tools: Cloud network/security services

Assessment: Network design review

Portfolio evidence: Secure cloud network diagram

04 Data, Secrets and Key Security

8 hours

TOPICS

Classification · Encryption · KMS/key vaults · Secrets management · Rotation · Storage policies · Database controls · Tokenisation concepts · Backup protection

PRACTICAL WORK

Implement a secrets and encryption strategy for application/data services.

Tools: KMS/Key Vault/Secret Manager concepts

Assessment: Data security lab

Portfolio evidence: Cloud data protection design

CURRICULUM

Course curriculum

8 modules · 8 weeks · 78 hours of guided learning

05 Workload, Container and Serverless Security

10 hours

TOPICS

VM hardening · Images · Containers · Kubernetes security concepts · Serverless permissions · Runtime controls · Supply chain · Vulnerability management

PRACTICAL WORK

Assess a containerised workload and design preventive/detective controls.

Tools: Container scanner concepts, Kubernetes security controls

Assessment: Workload review

Portfolio evidence: Cloud workload hardening plan

06 DevSecOps, CSPM and Cloud Posture

10 hours

TOPICS

IaC scanning · Policy-as-code · CI/CD security · CSPM/CNAPP concepts · Misconfiguration detection · Compliance mapping · Remediation workflows

PRACTICAL WORK

Add IaC/container scanning and posture checks to a deployment pipeline.

Tools: Terraform, CI/CD, CSPM/CNAPP concepts

Assessment: DevSecOps lab

Portfolio evidence: Secure cloud deployment pipeline



CURRICULUM

Course curriculum

8 modules · 8 weeks · 78 hours of guided learning

07 Cloud Detection, Incident Response and Forensics

10 hours

TOPICS

Cloud audit logs · Identity events · Workload telemetry · Detection use cases · Compromised credentials · Isolation · Snapshots · Evidence · Recovery

PRACTICAL WORK

Investigate a simulated cloud account compromise and execute a response playbook.

Tools: Cloud audit/monitoring logs, SIEM concepts

Assessment: Cloud IR practical

Portfolio evidence: Cloud incident response report

08 Governance, Compliance and Cloud Security Capstone

16 hours

TOPICS

Control frameworks · Policies · Continuous compliance · Risk · Third parties · Data residency · Architecture review · Cost/security balance · Executive communication

PRACTICAL WORK

Secure an end-to-end cloud application and present architecture, controls, detections and incident plan.

Tools: AWS/Azure/GCP security services, IaC, SIEM concepts

Assessment: Capstone defence

Portfolio evidence: Cloud security architecture portfolio

APPLIED PORTFOLIO

Projects you will build

Two portfolio projects supported by guided module work.

PORTFOLIO PROJECT 1

Secure Cloud Application Blueprint

Harden IAM, network, data, workloads and CI/CD for a cloud application.

DELIVERABLES

Threat model · IaC/security controls · Logging · Incident plan

PORTFOLIO PROJECT 2

Cloud Compromise Investigation

Investigate a simulated compromise of an identity or workload and carry out the response.

DELIVERABLES

Evidence timeline · Containment steps · Root cause · Improvements

LEARNING EXPERIENCE

Learn, practise and present

- Live instructor-led sessions that connect concepts to real workplace decisions.
- Guided labs and workshops in every module.
- Assignments, checkpoints and practical feedback.
- Portfolio documentation, demonstrations and capstone review.
- Access to recordings and LMS resources according to the published batch policy.
- Career preparation based on completed work and target roles.

Tools you will work with

Cloud architecture tools · AWS · Azure · GCP IAM concepts · Cloud network/security services · KMS · Key Vault · Secret Manager concepts · Container scanner concepts · Kubernetes security controls · Terraform · CI/CD · CSPM · CNAPP concepts

CAREER PREPARATION

Build confidence for interviews

A structured process to connect your learning with your next career step.

01**Role clarity**

Identify roles that fit your background, interests and current skills.

02**Profile readiness**

Review your CV, LinkedIn, GitHub and project summaries.

03**Project proof**

Prepare to demonstrate completed work and explain your decisions.

04**Interview practice**

Practise technical questions, project walkthroughs and interviews.

05**Opportunity updates**

Receive relevant job openings and employer requirements, subject to availability and learner readiness.

Career support helps you prepare. Employment outcomes depend on experience, project quality, interview readiness and market conditions.

LEARNER JOURNEYS

Companies where our learners have been hired

Across the Brightnest AI Academy learner community



Learner employment history across the academy; not a placement guarantee for this course. Names and logos identify employers; they do not imply endorsement or a hiring partnership.

BEFORE YOU ENROL

Your questions, answered

Is the Cloud Security Engineering course suitable for beginners?

This is an advanced-level course. Learners should understand cloud and cybersecurity fundamentals. Prior exposure to AWS, Azure, or Google Cloud is helpful.

What will I build during the course?

You will complete guided labs in every module and build two portfolio projects: Secure Cloud Application Blueprint and Cloud Compromise Investigation. Deliverables include working files or code, documentation, testing or evaluation evidence, and a final presentation.

Which tools and platforms are covered?

Key tools include Cloud architecture tools, AWS, Azure, GCP IAM concepts, Cloud network, security services, KMS, and Key Vault. Additional platforms are introduced in relevant modules through practical tasks, and the toolset may evolve as industry practice changes.

How long does the course take?

The course includes approximately 78 guided learning hours across 8 modules, delivered over 8 weeks.

Which career paths can this course support?

The curriculum supports the development of skills relevant to roles such as Cloud Security Engineer, DevSecOps Engineer, and Cloud Security Analyst. Career outcomes depend on prior experience, project quality, interview readiness and market conditions; employment is not guaranteed.

BEFORE YOU ENROL

Your questions, continued

Will I receive mentor and career support?

The course includes live instruction, lab support, assignment feedback, project reviews and career preparation covering portfolio development, CV writing, LinkedIn profile improvement, and interview guidance.

FEES & ADMISSIONS

Plan your next step

COURSE FEE

INR 35,000 + GST

EMI and easy instalments available

Duration	8 weeks
Level	Advanced
Learning format	Live mentor-led learning
Batch starts	Expected Saturday / Sunday starts

Check the live Batches page for the next expected weekend. Confirm the exact date, class times and availability with admissions.

Book a free demo class >

+91 73030 11395

brightnestaiacademy.com/batches

A-56, Sector-64, Noida, Uttar Pradesh - 201301