# Forebrain — Cloud Security & DevSecOps (3 Months / 12 Weeks)

Duration: 3 Months (12 Weeks / 60 instructional days)

Format: 1 hour class + 1 hour lab practice (Monday–Friday). Saturday = Activity Day (practical session based on weekly topics).

Focus: Practical hands-on implementation of secure cloud architecture, DevSecOps automation, and compliance across AWS, Azure, and GCP.

Outcome: Students will build secure cloud environments, automate DevSecOps pipelines, and complete a capstone project integrating multi-cloud security automation.

## Phase 1 — Cloud Security Foundations & Architecture (Weeks 1–3)

- Introduction to Cloud Computing models: IaaS, PaaS, SaaS, and shared responsibility model

- Understanding core services: Compute (EC2), Storage (S3), Networking (VPC), IAM fundamentals

- Identity and Access Management (IAM): roles, policies, and permissions management

- Cloud networking and segmentation best practices (VPCs, subnets, NACLs, SGs)

- Encryption and key management (KMS, Azure Key Vault, Google KMS)

- Cloud auditing and logging: AWS CloudTrail, Azure Monitor, GCP Cloud Logging

- Cloud compliance frameworks (CIS, NIST, ISO 27017) and introduction to CIS benchmarks

Deliverable: Secure baseline architecture with IAM policy and VPC segregation setup

## Phase 2 — Cloud Security Assessment & Hardening (Weeks 4–6)

- Cloud security auditing tools: ScoutSuite, Prowler, CloudSploit overview

- Automated vulnerability scanning and remediation workflows

- Penetration testing in the cloud (AWS penetration testing guidelines)

- Container security: Docker, Trivy, Dockle — image scanning and hardening

- Kubernetes security concepts and auditing using kube-bench and kube-hunter

- Implementing least privilege and identity federation (SSO, SAML, IAM roles)

- Incident detection using AWS GuardDuty, Azure Defender, GCP Security Command Center

Deliverable: Cloud assessment report + hardened infrastructure using automation scripts

## Phase 3 — DevSecOps Implementation & CI/CD Security (Weeks 7–9)

- DevOps vs. DevSecOps — core concepts and architecture flow

- Integrating security into CI/CD pipelines (Jenkins, GitHub Actions)

- Static code analysis (SAST) with SonarQube and Snyk

- Dynamic application security testing (DAST) using OWASP ZAP automation

- Container image signing and verification in CI/CD

- Infrastructure as Code (IaC) — securing Terraform, Ansible, and CloudFormation

- Secrets management in pipelines: HashiCorp Vault, AWS Secrets Manager, GitHub secrets

Deliverable: Secure CI/CD pipeline with integrated security scans and secret management

## Phase 4 — Compliance, Monitoring & Capstone (Weeks 10–12)

- Continuous compliance with AWS Config, Azure Policy, and GCP Security Command Center

- Security monitoring dashboards with CloudWatch, Azure Monitor, and ELK integration

- Automated incident response with Lambda and Azure Logic Apps

- Security policy-as-code implementation (OPA, Terraform Cloud Policies)

- Multi-cloud security architecture design and governance controls

- Capstone: Secure Multi-Cloud Infrastructure Deployment with Automated DevSecOps Pipeline

- Final project presentation and security audit report submission

Deliverable: Capstone project report + secure automated DevSecOps infrastructure build

## Tools & Technologies Covered

Cloud Platforms:

- AWS

- Azure
- Google Cloud Platform (GCP)

Security & Assessment:

- ScoutSuite
- Prowler
- CloudSploit
- Pacu
- Burp Suite

Container & K8s:

- Docker
- Trivy
- Dockle
- kube-bench
- kube-hunter

DevSecOps CI/CD:

- Jenkins
- GitHub Actions
- GitLab CI
- Snyk
- SonarQube

Infrastructure as Code:

- Terraform
- Ansible
- CloudFormation

Monitoring & Compliance:

Forebrain — Cloud Security & DevSecOps (3-Month Syllabus)

- AWS Config
- Azure Defender
- GCP SCC
- ELK Stack
- Grafana

## Deliverables & Assessment

- Phase-wise cloud security lab exercises and automation scripts
- Hardening and vulnerability management reports
- Secure CI/CD pipeline with integrated DevSecOps checks
- Cloud compliance and monitoring dashboard configuration
- Capstone project: Secure Multi-Cloud Deployment with Automated Security Validation