■ 30-Day AWS DevSecOps Training Programme

Phase 1: Foundations (Day 1–5) – Linux + Git + Basics

- Day 1: Linux Basics – Commands, file system, users & groups, permissions (Lab: Manage users & file permissions).
- Day 2: Linux Advanced & Shell Scripting – Processes, services, cron jobs, package management (Lab: Write a script to monitor disk usage).
- Day 3: Git Fundamentals – Git workflow, branching, merging (Lab: Push/pull from GitHub/GitLab).
- Day 4: GitHub/GitLab Actions Basics – Intro to CI/CD with GitHub Actions & GitLab CI (Lab: Create a simple pipeline).
- Day 5: Security in Git – Secret scanning, signed commits, GitGuardian (Lab: Detect & remediate leaked secrets).

Phase 2: DevOps Tools & AWS Basics (Day 6–10)

- Day 6: AWS Core Services – IAM, VPC, EC2, S3 basics (Lab: Launch EC2 with security groups).
- Day 7: Docker – Containerization, Dockerfiles, image scanning (Tools: Trivy). (Lab: Build & scan a Docker image).
- Day 8: Kubernetes (EKS) Basics – Pods, deployments, services (Tools: Kubescape, Kube-bench). (Lab: Deploy app on EKS with pod security policies).
- Day 9: Jenkins / GitHub Actions / GitLab CI – CI/CD pipelines with security gates (Lab: Build Maven app → Docker → push to ECR).
- Day 10: IaC Basics (Terraform/CloudFormation) – Secure infra provisioning (Tools: Checkov, TFSec). (Lab: Scan Terraform templates).

Phase 3: Security Tools (Day 11–20)

- Day 11: SAST – Tools: SonarQube, Semgrep (Lab: Integrate SAST into CI/CD).
- Day 12: DAST – Tools: OWASP ZAP (Lab: Test a running app).
- Day 13: Dependency/Artifact Scanning – Tools: OWASP Dependency-Check, Snyk (Lab: Scan dependencies).
- Day 14: Container Security – Tools: Trivy, Anchore (Lab: Block vulnerable images).
- Day 15: Secrets Management – Tools: AWS Secrets Manager, Vault (Lab: Store & retrieve secrets).
- Day 16: Cloud Security – Tools: Prowler, ScoutSuite (Lab: Audit AWS account security).
- Day 17: Policy-as-Code – Tools: OPA, Conftest (Lab: Enforce policies in pipelines).
- Day 18: Logging & Monitoring – Tools: CloudWatch, GuardDuty, ELK/EFK (Lab: Detect anomalous activity).
- Day 19: Vulnerability Management – Tools: Nessus, AWS Inspector (Lab: Scan EC2 for vulnerabilities).
- Day 20: Threat Modeling & Shift-Left Security – STRIDE & threat analysis (Lab: Apply threat modeling).

Phase 4: End-to-End DevSecOps Pipeline (Day 21–30)

- Day 21: Pipeline Orchestration – GitHub/GitLab Actions with security gates (Lab: Create pipeline with SAST + DAST).
- Day 22: Integrating IaC Security – Add Terraform scanning (Lab: Fail builds if misconfigurations found).
- Day 23: Integrating Container Security – Add Trivy scans (Lab: Block vulnerable images).
- Day 24: Integrating K8s Security – Add Kubescape checks (Lab: Fail pipeline if pod security policies fail).

- Day 25: AWS Security Automation – Automate audits with Prowler + GuardDuty.
- Day 26: Continuous Monitoring & Alerts – Setup alerts with CloudWatch + Slack/MS Teams.
- Day 27: Incident Response Simulation – Hands-on response to simulated pipeline attack.
- Day 28: End-to-End Project Setup – Deploy secure app via CI/CD → EKS → monitoring.
- Day 29: Group Project – Teams design & implement secure DevOps pipeline.
- Day 30: Review & Assessment – Evaluation, Q&A;, certification prep.

■ Tools Covered

- **Version Control & CI/CD** → GitHub, GitLab, Jenkins - **SAST/DAST** → SonarQube, Semgrep, OWASP ZAP - **Dependency/Container Security** → Trivy, Snyk, Anchore - **Cloud Security** → Prowler, ScoutSuite, AWS Inspector, GuardDuty - **IaC Security** → TFSec, Checkov, OPA - **Secrets Management** → Vault, AWS Secrets Manager - **Monitoring** → ELK/EFK, CloudWatch