

# Certified DevSecOps Professional with AWS - 40 Hour TOC

## Course Prerequisites

Participants should have:

- Basic Linux and CLI experience
- Understanding of CI/CD pipelines (Git, Jenkins/GitLab CI/GitHub Actions)
- Familiarity with AWS core services (EC2, S3, IAM, VPC)
- Basic scripting knowledge (Shell/Python preferred)
- (Optional) Prior DevOps or Security background

## Week 1: Foundations & AWS Security Core (10 Hours)

Day 1: DevSecOps Introduction & AWS IAM (4h)

Theory (2h):

- What is DevSecOps? Pillars of DevSecOps
- Traditional vs Modern security practices in CI/CD
- AWS Shared Responsibility Model
- AWS IAM: Users, Roles, Policies, STS

Labs (2h):

- Creating IAM users, groups, policies
- IAM least privilege demo
- Role assumption and IAM Access Analyzer

Day 2: Secrets Management & Secure Networking (6h)

Theory (2h):

- AWS Secrets Manager, Parameter Store (SSM)
- VPC security: NACLs, Security Groups, Flow Logs
- Best practices: Encryption in-transit/at-rest

Labs (4h):

- Store & rotate secrets using AWS Secrets Manager
- Build secure VPC: public/private subnets, NACLs, SGs

# Certified DevSecOps Professional with AWS - 40 Hour TOC

- Enable VPC Flow Logs & analyze with Athena

## Week 2: CI/CD Security & Static/Dynamic Analysis (10 Hours)

### Day 3: Secure CI/CD Pipelines (5h)

#### Theory (2h):

- Security in the pipeline stages
- Threat modeling & SBOM in CI
- AWS CodePipeline + CodeBuild/CodeDeploy security
- Using Git Hooks for security enforcement

#### Labs (3h):

- Build a secure CodePipeline with CodeBuild
- Integrate role-based access for CI/CD
- Git hooks + commit signature enforcement

### Day 4: Static & Dynamic Scanning (5h)

#### Theory (2h):

- SAST vs DAST vs SCA
- OWASP Top 10 explained
- Security tooling options: SonarQube, Trivy, Bandit

#### Labs (3h):

- Run Trivy to scan containers in CodeBuild
- Use SonarQube for code analysis
- Integrate Bandit for Python code linting

## Week 3: Container Security & Kubernetes (10 Hours)

### Day 5: Container Security (5h)

#### Theory (2h):

- Dockerfile hardening & image signing (cosign/sigstore)

# Certified DevSecOps Professional with AWS - 40 Hour TOC

- Registry security (ECR) and scanning
- Seccomp, AppArmor, capabilities

Labs (3h):

- Harden Dockerfile and build secure images
- Scan ECR with AWS Inspector v2
- Image signing using cosign + verify before deploy

Day 6: Kubernetes Security (EKS Focus) (5h)

Theory (2h):

- EKS architecture and RBAC
- Pod security: PSPs, PodSecurityAdmission
- Network policies, audit logs, IAM Roles for Service Accounts (IRSA)

Labs (3h):

- Create secure EKS cluster with IRSA
- Apply NetworkPolicy & scan workloads using Kubescape or Kube-bench
- Integrate OPA/Gatekeeper for policy-as-code

## Week 4: Monitoring, Logging, and Incident Response (10 Hours)

Day 7: Security Monitoring & Logging (5h)

Theory (2h):

- AWS GuardDuty, CloudTrail, Config, Security Hub
- Open source SIEM & Alerting basics
- Audit logging and centralized log analysis

Labs (3h):

- Enable GuardDuty & configure Security Hub
- Analyze CloudTrail logs with Athena
- Set alerts on suspicious activities (e.g., Root account use)

# Certified DevSecOps Professional with AWS - 40 Hour TOC

## Day 8: Threat Detection & Response Automation (5h)

### Theory (2h):

- Security incident playbooks
- Automating remediation (Lambda, EventBridge)
- Forensics basics on AWS

### Labs (3h):

- Simulate GuardDuty finding and auto-remediate via Lambda
- Build basic IR Lambda pipeline
- Archive forensic evidence using S3 + KMS

## Capstone Project & Certification Prep (Final Day - 5 Hours)

### Capstone Project (3h):

- Build an end-to-end secure CI/CD pipeline:
  - Store secret in Secrets Manager
  - Harden Docker image + scan + deploy to EKS
  - Enable GuardDuty + auto-remediation
  - Use IAM roles, encryption, and logging

### Review & Mock Exam (2h):

- Review of core AWS DevSecOps concepts
- 30-question mock exam
- Q&A and certification guidance

## Tools Covered

AWS: IAM, VPC, S3, Secrets Manager, ECR, CodePipeline, CodeBuild, CloudTrail, GuardDuty, Security Hub, Lambda

Open Source: Trivy, SonarQube, Bandit, Git Hooks, OPA/Gatekeeper, Kube-bench, Kubescape

CI/CD: GitHub Actions / GitLab CI / Jenkins (depending on setup)

# **Certified DevSecOps Professional with AWS - 40 Hour TOC**

Security Concepts: OWASP, SBOM, RBAC, IRSA, CIS Benchmarks