DevSecOps

Build security into every stage of CI/CD, from code and dependencies to containers and cloud.

DURATION	FORMAT	LEVEL	LABS
45 hours	Onsite, online or hybrid	Advanced	Cloud sandbox included

About this programme

An advanced, demo-led programme that embeds security across the delivery pipeline: SAST, DAST and dependency scanning, secrets detection, IaC and container security, Kubernetes hardening, Vault-based secrets management and cloud security controls.

Who it is for: DevOps engineers, developers, SREs and application security engineers

What your team will be able to do

- Integrate SAST, DAST and dependency scanning into CI/CD pipelines
- Enforce protected branches, pre-merge checks and secrets detection
- Scan container images and harden Kubernetes deployments
- Manage secrets with HashiCorp Vault in pipelines
- Apply cloud controls: IAM, network rules, WAF, KMS and DDoS protection

Before you start

- Experience with CI/CD pipelines
- Docker; Kubernetes basics help
- Working knowledge of one programming language

Course outline

1. From DevOps to DevSecOps

- SDLC, DevOps and infrastructure as code
- Why DevSecOps: security at every stage of the SDLC
- CI/CD workflows for developers and testers
- Key terminology: NVD, CVE and CPE
- Security checklists

2. Securing code and dependencies

- Static analysis with SonarQube and Snyk
- Code quality and security hotspots
- Third-party dependency scanning with OWASP Dependency-Check
- Protected branches and pre-merge checks
- Secrets detection with Gitleaks and other linters

3. Dynamic testing and artefacts

- Dynamic security testing with OWASP ZAP
- Demo: DAST in a pipeline
- Artefact repository scanning
- Writing secure IaC and testing it with Chef InSpec

4. Containers and Kubernetes

- Image scanning with Trivy, Snyk, Twistlock and Docker's native scanner
- Kubernetes security assessment with kube-bench
- Secure deployments: security contexts, network policies and RBAC

5. Secrets, infrastructure and cloud security

- HashiCorp Vault: local use and pipeline integration
- VM security with Qualys and native cloud tools
- Cloud security: IAM, security groups, NSGs, WAF and L4/L7 controls
- Encryption with KMS: customer-managed and cloud-managed keys
- DDoS prevention

Sample schedule

6 days onsite, or 12 half-day sessions online. We fit days and session lengths to your team's calendar.

Day 1	8 h	From DevOps to DevSecOps
Day 2	8 h	From DevOps to DevSecOps (continued); Securing code and dependencies
Day 3	8 h	Securing code and dependencies (continued); Dynamic testing and artefacts
Day 4	8 h	Dynamic testing and artefacts (continued); Containers and Kubernetes
Day 5	8 h	Containers and Kubernetes (continued); Secrets, infrastructure and cloud security
Day 6	5 h	Secrets, infrastructure and cloud security (continued)

Assessment and certification

How learning is checked

- A short knowledge check on day one and again at the end, so you can see each person's progress
- Graded hands-on labs in every module, reviewed by the trainer
- A final exercise that applies the programme to a problem like your team's own

Certificate and exams

- Participants who complete the programme receive a Cognitive Networks AI certificate of completion.

Formats and cohort size

- Onsite: At your office or a venue you choose, in full days.
- Online, live: Instructor-led over video, usually in half-day sessions so people can keep up with work.
- Hybrid: Some days in a room together, the rest online. Useful when a team works across cities.

Cohort size: 15 to 25 people per trainer. Larger teams run as parallel cohorts on the same outline, so everyone learns the same thing.

Pricing: We quote per cohort, based on duration, format and number of cohorts. There is no per-seat price list: tell us your team and we send a proposal within one business day.

Bring this programme to your team

Request a proposal at cognitivenetworks.ai/contact?programme=devsecops

reachus@cognitivenetworks.ai · Bangalore +91 72043 05303 · Dallas +1 (303) 827-7415