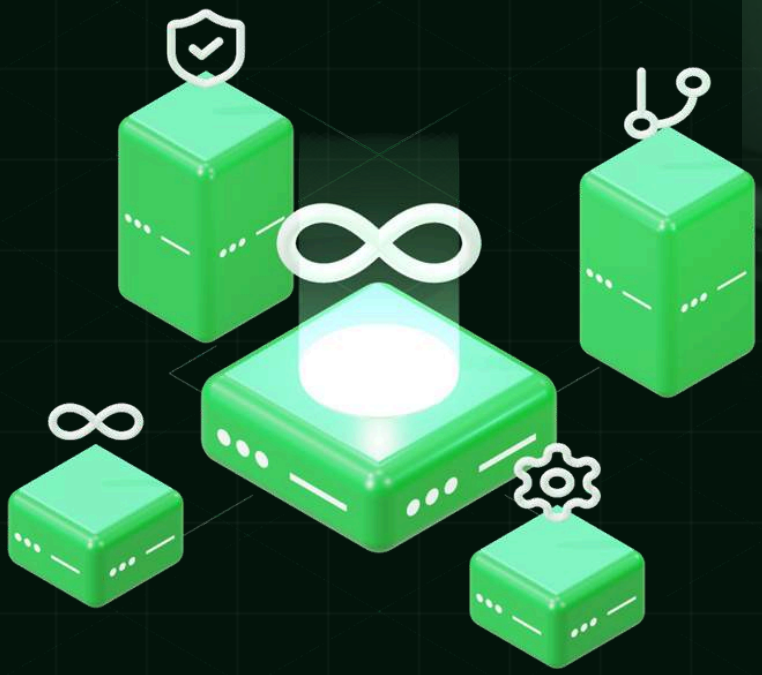
✦ DEVOPS & PLATFORM ENGINEERING · ADVANCED

DevSecOps — Security in DevOps Pipelines

Ship fast. Ship secure.





72	8	SAM-DEVSECOPS
HOURS	MODULES	CERTIFICATION

✦ INSIDE THIS BROCHURE

Contents

Program overview 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

Tools & platforms 10

Projects & capstone 11

Certification & method 12

Learning path 13

FAQs 14



AT A GLANCE

Level	Advanced
Duration	72 Hours
Modules	8
Certificate	SAM-DEVSECOPS

✦ PROGRAM OVERVIEW

Ship fast. Ship secure.



Embed security across the DevOps pipeline — scanning, secrets, supply chain and policy as code.

Fast delivery only works when security moves at the same speed, built into every commit, build and deployment rather than added at the end. This advanced program shows how to embed threat modelling, SAST, SCA, secret detection, container and infrastructure scanning, software supply chain controls, DAST and policy as code into CI/CD pipelines and Kubernetes, guided by OWASP and SLSA practices.

LEVEL	DURATION	CERTIFICATION	DELIVERY
Advanced	72 Hours	SAM-DEVSECOPS	Instructor-led · Live virtual · Blended



✦ WHAT YOU'LL PRACTISE

Integrate security scans into pipelines	01
Manage secrets safely	02
Secure the software supply chain	03
Enforce policy as code	04

✦ WHO IT'S FOR

Built for people ready to grow.

01

Developers & sysadmins

DevOps, Linux and Git foundations

02

DevOps engineers

Docker, Kubernetes, Terraform, CI/CD

03

Platform teams

GitOps, Helm, Backstage, observability

04

Reliability leads

SRE practices and DevSecOps

PREREQUISITES

Hands-on CI/CD experience with Jenkins or GitHub Actions	01
Working knowledge of Docker and Kubernetes	02
Basic understanding of application security concepts	03

ROLES YOU CAN TARGET

- DevSecOps Engineer ↗
- Application Security Engineer ↗
- Cloud Security Engineer ↗
- Security-focused DevOps Engineer ↗
- Product Security Team Member ↗
- Platform Security Engineer ↗

✦ LEARNING OUTCOMES

What you'll be able to do.

01 Integrate SAST, SCA and secret scanning into CI pipelines

02 Threat model applications and pipelines using STRIDE methodology

03 Secure containers, images and Kubernetes workloads against misconfiguration

04 Manage secrets with Vault and short-lived cloud credentials

05 Secure the software supply chain with SBOMs and signing

06 Enforce security policy as code across infrastructure and clusters

HOURS PER MODULE



✦ PROGRAM RUNWAY

Your journey, module by module.

8
MODULES · 72 HRS

01	**DevSecOps Principles and Threat Modelling** Shift-left and shared responsibility, Secure SDLC practices, OWASP Top 10 overview	8 hrs
02	**Securing Source Code** SAST with Semgrep and SonarQube, Secret detection with Gitleaks, Pre-commit hooks	10 hrs
03	**Dependency and Supply Chain Security** Software composition analysis, Dependabot and OWASP Dependency-Check, SBOM generation with Syft	10 hrs
04	**Container and Image Security** Minimal and distroless images, Scanning with Trivy and Grype, Dockerfile linting with Hadolint	8 hrs
05	**Secrets Management** Risks of hardcoded secrets, HashiCorp Vault fundamentals, Dynamic secrets	8 hrs
06	**Infrastructure as Code Security** Misconfiguration risks in cloud, Scanning Terraform with Checkov, tfsec and Trivy config scanning	8 hrs
07	**Kubernetes and Runtime Security** Pod Security Standards, RBAC and network policies, Admission control with Kyverno and OPA Gatekeeper	10 hrs
08	**DAST, Policy and Security Operations** DAST with OWASP ZAP, Policy as code with Open Policy Agent, Security gates and risk acceptance	10 hrs
★	**Capstone · End-to-End Secure Delivery Pipeline** Assessment, capstone review and certification	

✦ DETAILED CURRICULUM

The syllabus.

Modules 01–03

MODULE 01

DevSecOps Principles and Threat Modelling

8 hours

Hands-on lab
Threat model a sample application and its CI/CD pipeline using STRIDE.

TOPICS COVERED

- Shift-left and shared responsibility
- Secure SDLC practices
- OWASP Top 10 overview
- STRIDE threat modelling
- OWASP DevSecOps maturity model
- Security champions programs

OWASP

MODULE 02

Securing Source Code

10 hours

Hands-on lab
Add Semgrep and Gitleaks checks that block insecure code on pull requests.

TOPICS COVERED

- SAST with Semgrep and SonarQube
- Secret detection with Gitleaks
- Pre-commit hooks
- Branch protection and signed commits
- Triage of false positives

MODULE 03

Dependency and Supply Chain Security

10 hours

Hands-on lab
Generate an SBOM, sign an image with Cosign and verify the signature.

TOPICS COVERED

- Software composition analysis
- Dependabot and OWASP Dependency-Check
- SBOM generation with Syft
- Image signing with Sigstore Cosign
- SLSA framework levels
- Provenance attestations

OWASP

LEARN BY DOING

8 guided labs, one in every module.

✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 04–06

MODULE 04

Container and Image Security

8 hours

Hands-on lab
Harden a Dockerfile and fail builds on critical Trivy findings.

TOPICS COVERED

- Minimal and distroless images
- Scanning with Trivy and Grype
- Dockerfile linting with Hadolint
- Non-root and read-only containers
- Registry security policies

MODULE 05

Secrets Management

8 hours

Hands-on lab
Replace pipeline credentials with Vault dynamic secrets and OIDC authentication.

TOPICS COVERED

- Risks of hardcoded secrets
- HashiCorp Vault fundamentals
- Dynamic secrets
- OIDC workload identity in CI
- Kubernetes secrets and External Secrets Operator

Kubernetes

MODULE 06

Infrastructure as Code Security

8 hours

Hands-on lab
Scan Terraform code with Checkov and remediate high-severity misconfigurations.

TOPICS COVERED

- Misconfiguration risks in cloud
- Scanning Terraform with Checkov
- tfsec and Trivy config scanning
- Least-privilege IAM design
- Drift and compliance checks

Terraform

LEARN BY DOING

8 guided labs, one in every module.



✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 07–08

MODULE 07

Kubernetes and Runtime Security

10 hours

Hands-on lab
Enforce Kyverno policies and detect suspicious container behaviour with Falco.

TOPICS COVERED

- Pod Security Standards
- RBAC and network policies
- Admission control with Kyverno and OPA Gatekeeper
- Runtime detection with Falco
- CIS benchmarks with kube-bench

Kubernetes

MODULE 08

DAST, Policy and Security Operations

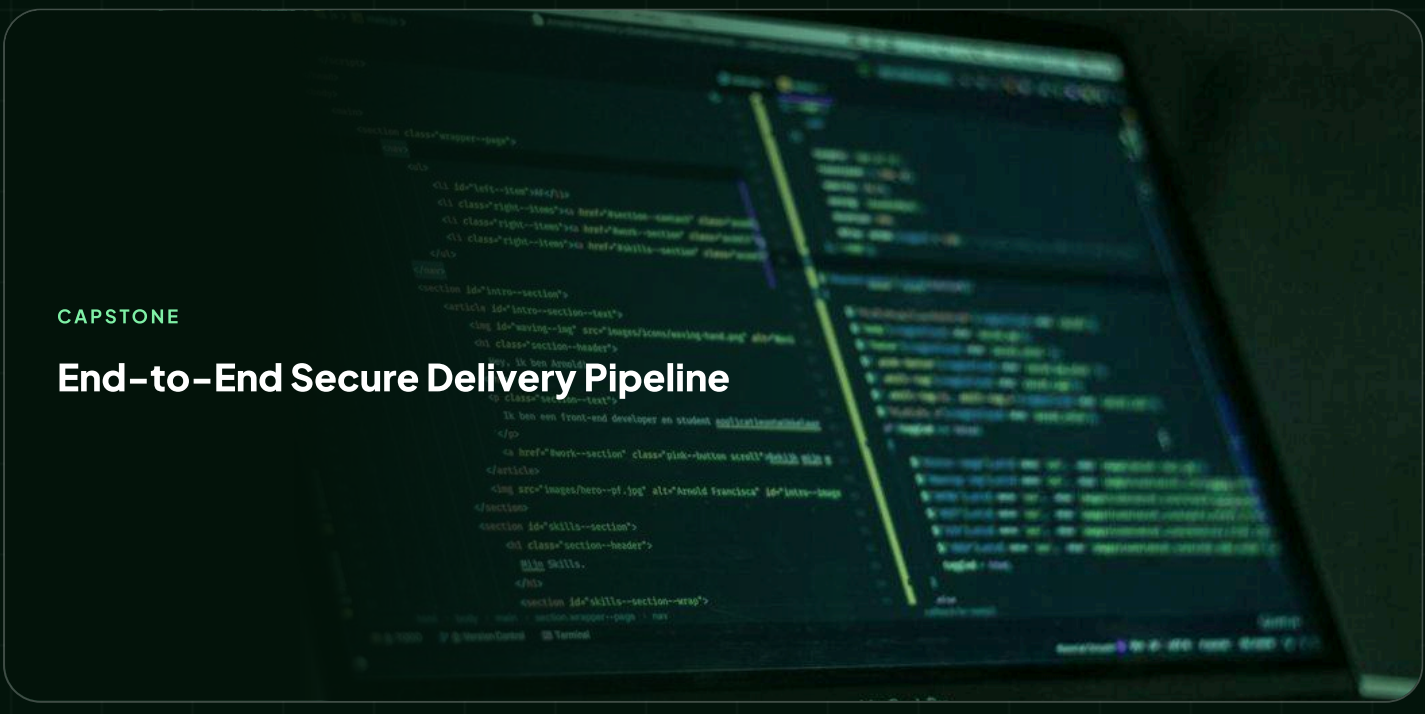
10 hours

Hands-on lab
Run an automated OWASP ZAP baseline scan as a staging deployment gate.

TOPICS COVERED

- DAST with OWASP ZAP
- Policy as code with Open Policy Agent
- Security gates and risk acceptance
- Vulnerability management workflows
- Security metrics and reporting
- Incident response in pipelines

OWASP



CAPSTONE

End-to-End Secure Delivery Pipeline

✦ YOUR STACK

Tools you'll build with.

Real platforms and frameworks — the same stack modern teams ship with, practised in cloud-hosted labs.

GitHub
Code hosting & Actions CI

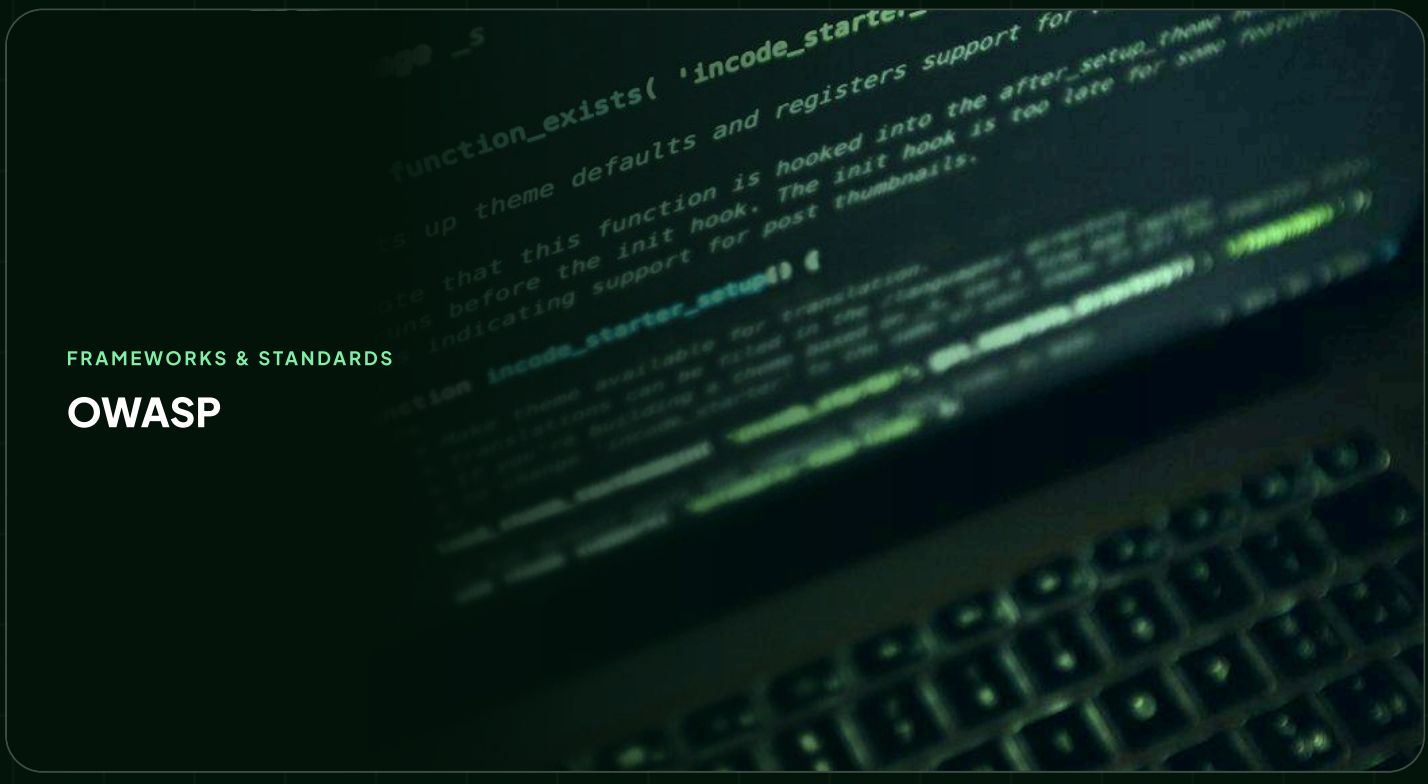
Docker
Containers & images

Kubernetes
Container orchestration

Jenkins
CI/CD pipelines

OWASP
Top 10 & testing standards

Terraform
Infrastructure as code



FRAMEWORKS & STANDARDS

OWASP

✦ HANDS-ON WORK

Projects that prove you can do it.

01

Secure CI Pipeline

Build a pipeline integrating Semgrep, Gitleaks, dependency scanning and Trivy with clear pass, warn and fail security gates.

02

Supply Chain Integrity

Generate SBOMs, sign images with Cosign, record provenance attestations and verify signatures before deployment to Kubernetes.

03

Kubernetes Policy Guardrails

Implement Kyverno or Gatekeeper policies blocking privileged pods, unsigned images and missing resource limits, with Falco runtime alerts.

CAPSTONE PROJECT

End-to-End Secure Delivery Pipeline

Secure a microservices application from commit to runtime: threat model, SAST, SCA, secret detection, IaC and image scanning, signed images with SBOMs, Vault-managed secrets, Kubernetes admission policies, DAST gates and a remediation report.

Real-world scenario | Mentor review | Portfolio ready



CERTIFICATION

SAM-DEVSECOPS

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



✦ HOW YOU LEARN

The SAM Learning Framework™

PHASE 01

S

Scenario

Real-world attack and use-case scenarios open every module.

PHASE 02

A

Apply

Hands-on lab work, CTF challenges and live projects.

PHASE 03

M

Master

Assessment, peer review and certification prep.

PHASE 04

M

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive
- Hackathon / CTF
- Mentorship

✦ LEARNING PATH · DEVOPS & PLATFORM ENGINEERING

Where this program fits.

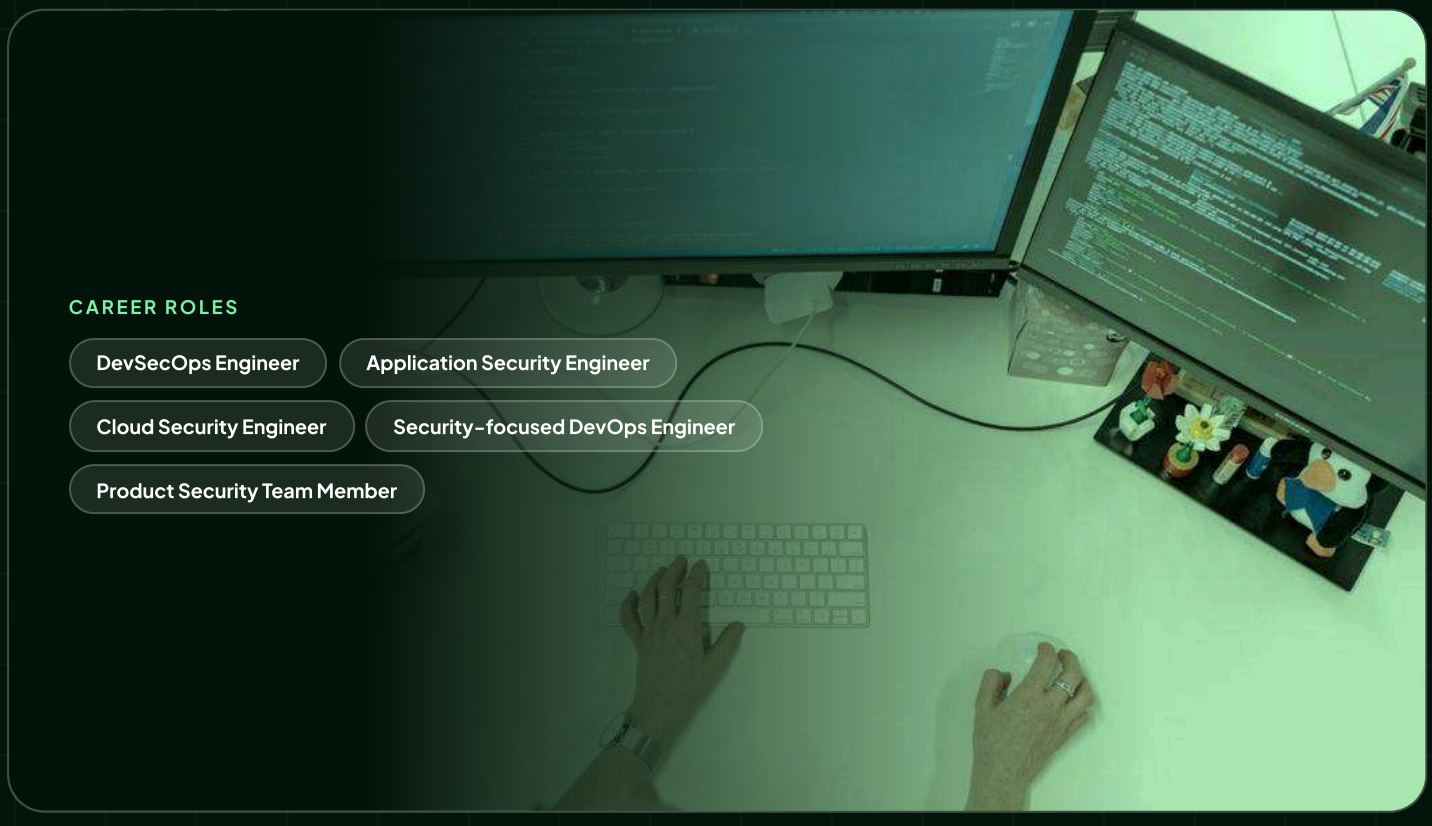
Beginner	Intermediate	Advanced	Expert
3 programs	6 programs	You are here	1 programs

BEFORE THIS

Docker Mastery	48 Hours
Kubernetes — From Zero to Hero	80 Hours
Terraform & Infrastructure as Code	56 Hours
Jenkins CI/CD Pipelines	48 Hours

UP NEXT

SRE — Site Reliability Engineering	80 Hours



CAREER ROLES

- DevSecOps Engineer
- Application Security Engineer
- Cloud Security Engineer
- Security-focused DevOps Engineer
- Product Security Team Member

✦ FAQS

Questions, answered.

Q01

Do I need prior experience to join?

This is an advanced program. You should have hands-on experience with CI/CD pipelines, Docker and Kubernetes, plus basic security awareness. Prior completion of our container or CI/CD courses, or equivalent work experience, is strongly recommended.

Q02

How is the program delivered and scheduled?

Sessions are instructor-led and run as live virtual classes or in a blended format. Batch timings, including weekday and weekend options, are confirmed at enrolment, and session recordings and notes support revision between classes.

Q03

What certification will I receive?

Learners who complete the required labs, projects and final assessments receive the Samcommunity Academy SAM-DEVSECOPS certificate. It records the skills you have demonstrated during the program and is awarded only after assessments are passed.

Q04

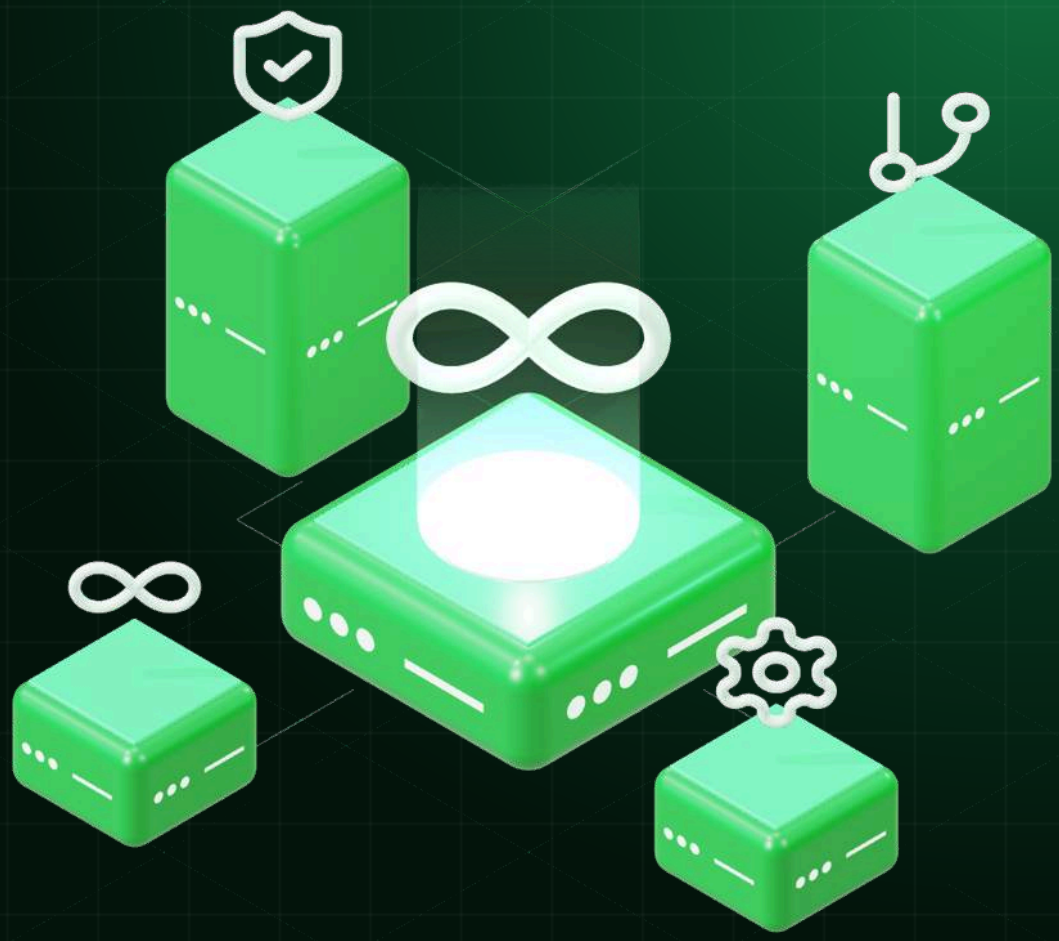
Will I get access to labs and tools?

Yes. You work with lab Git repositories, CI runners, a Kubernetes cluster and tools such as Semgrep, Gitleaks, Trivy, Cosign, Vault, Checkov, Kyverno, Falco and OWASP ZAP. Most are open source and can be run locally.

Q05

Does the program include career support?

You receive guidance on building a portfolio from your projects, resume and profile review, and mock interviews focused on DevSecOps, application security and cloud security roles. Career support helps you prepare, but jobs, interviews and salaries are not guaranteed.



✦ LET'S TALK

Start DevSecOps — Security in DevOps Pipelines with Samcommunity.

INDIVIDUALS

academy@samcommunity.in

Batches, enrolment & career guidance

CORPORATE & INSTITUTIONS

corporate@samcommunity.in

Team batches & custom programs

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India