Cloud & Application Security

Program Brochure · 2026

DEVSECOPS ESSENTIALS

Security built into every pipeline.

Intermediate

48 Hours

SAM-DSOE

Cybersecurity

Cloud & Application Security

8 programs in this track



6

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03
Who it's for 04
Learning outcomes 05
Program runway 06
Detailed curriculum 07
Tools & frameworks 09
Projects & capstone 10
Certification & method 11
Learning path 12
FAQs 13



AT A GLANCE

Level	**Intermediate**
Duration	**48 Hours**
Modules	**6**
Certificate	**SAM-DSOE**

Program overview

Security built into every pipeline.

Integrate security into CI/CD — code scanning, dependency checks, container security and policy as code.

Fast release cycles only stay safe when security is built into the pipeline rather than bolted on at the end. This program teaches you to integrate security into CI/CD, covering code and dependency scanning, container security and policy as code. You finish able to automate security checks in modern pipelines and help teams ship secure software without slowing delivery.

DELIVERY

Instructor-led · Live virtual · Blended



WHAT YOU'LL PRACTISE

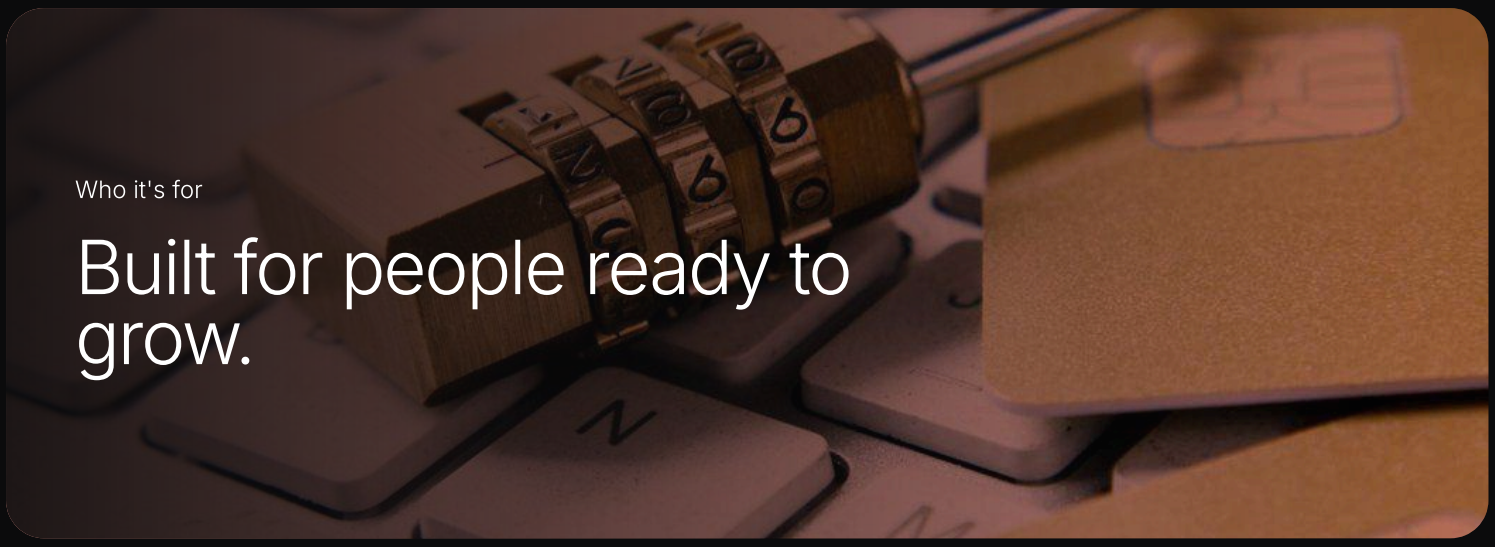
- Add SAST and dependency scanning to CI/C
- Scan containers and images
- Apply policy as code
- Build a security-first DevOps culture

LEVEL
Intermediate

DURATION
48 Hours

CERTIFICATION
SAM-DSOE

TRACK
Cloud & Application Security



Who it's for

Built for people ready to grow.

01

Fresh graduates & career switchers

Start with SOC-L1 or Ethical Hacking Fundamentals

02

SOC & IT teams

Level up to SIEM, EDR, DFIR and threat hunting

03

Pen testers & red teamers

Web, network, API, mobile and red-team programs

04

Security leaders

GRC, ISO 27001, risk and CISO leadership

PREREQUISITES

Basic understanding of software development	01
Familiarity with Git and CI/CD concepts	02
Comfort with the command line	03

ROLES THIS PREPARES YOU FOR

- DevSecOps Engineer ↗
- Application Security Engineer ↗
- Platform Engineer ↗
- CI/CD Pipeline Engineer ↗
- Site Reliability Engineer ↗
- Cloud Security Engineer ↗

Learning outcomes

What you'll be able to do.



01	Integrate SAST and dependency scanning into CI/CD pipelines
02	Scan containers and images for known vulnerabilities
03	Manage secrets securely across build and deploy pipelines
04	Apply policy as code to enforce security standards
05	Automate security gates without slowing down delivery
06	Foster a security-first culture across DevOps teams

Program runway

Module by module.

6
modules · 48 hours

01	**DevSecOps Foundations** DevSecOps principles, Shift-left security, CI/CD overview	8 hrs
02	**Secure Pipelines and Code Scanning** SAST integration, Dependency scanning, Secret detection	10 hrs
03	**Container and Image Security** Image scanning, Base image hygiene, Dockerfile best practices	8 hrs
04	**Secrets Management** Secrets in pipelines, Vault basics, Credential rotation	8 hrs
05	**Policy as Code** Policy as code concepts, Infrastructure scanning, Compliance gates	8 hrs
06	**Monitoring and Security Culture** Pipeline observability, Vulnerability metrics, Feedback loops	6 hrs
★	**Capstone · End-to-End Secure Pipeline** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

DevSecOps Foundations

8 hours

Hands-on lab
Map security checkpoints across a sample CI/CD pipeline

TOPICS COVERED

- DevSecOps principles
- Shift-left security
- CI/CD overview
- Pipeline threat points
- Tooling landscape
- Culture and collaboration

Module 02

Secure Pipelines and Code Scanning

10 hours

Hands-on lab
Add SAST and dependency scanning to a sample GitHub Actions pipeline

TOPICS COVERED

- SAST integration
- Dependency scanning
- Secret detection
- Pipeline configuration
- Quality gates
- Triage workflows

GitHub

Module 03

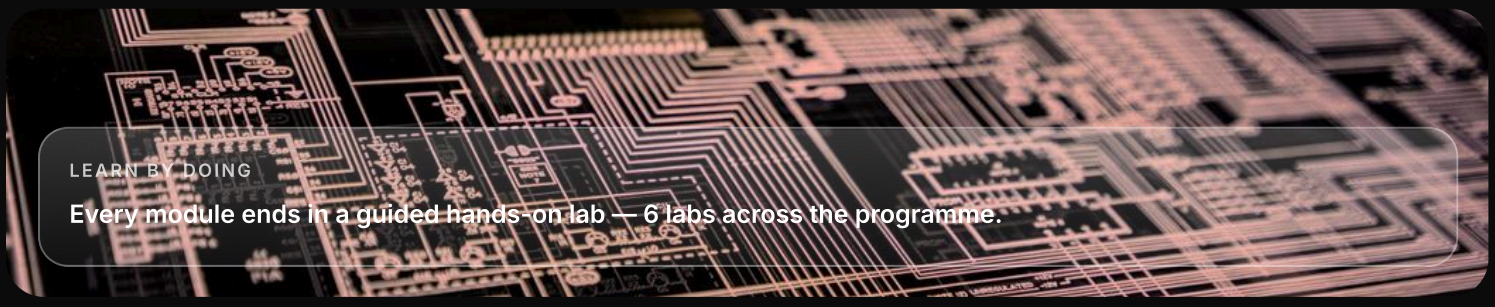
Container and Image Security

8 hours

Hands-on lab
Scan and harden a container image and fix flagged vulnerabilities

TOPICS COVERED

- Image scanning
- Base image hygiene
- Dockerfile best practices
- Registry security
- Runtime basics
- Supply chain awareness



Syllabus, continued.

Modules 04–06

Module 04

Secrets Management

8 hours

Hands-on lab
Integrate a secrets manager and remove hardcoded credentials from a pipeline

TOPICS COVERED

- Secrets in pipelines
- Vault basics
- Credential rotation
- Environment segregation
- Leak prevention
- Secure injection

Module 05

Policy as Code

8 hours

Hands-on lab
Enforce a policy-as-code rule that blocks an insecure configuration

TOPICS COVERED

- Policy as code concepts
- Infrastructure scanning
- Compliance gates
- Guardrail design
- Admission policies
- Exceptions handling

Module 06

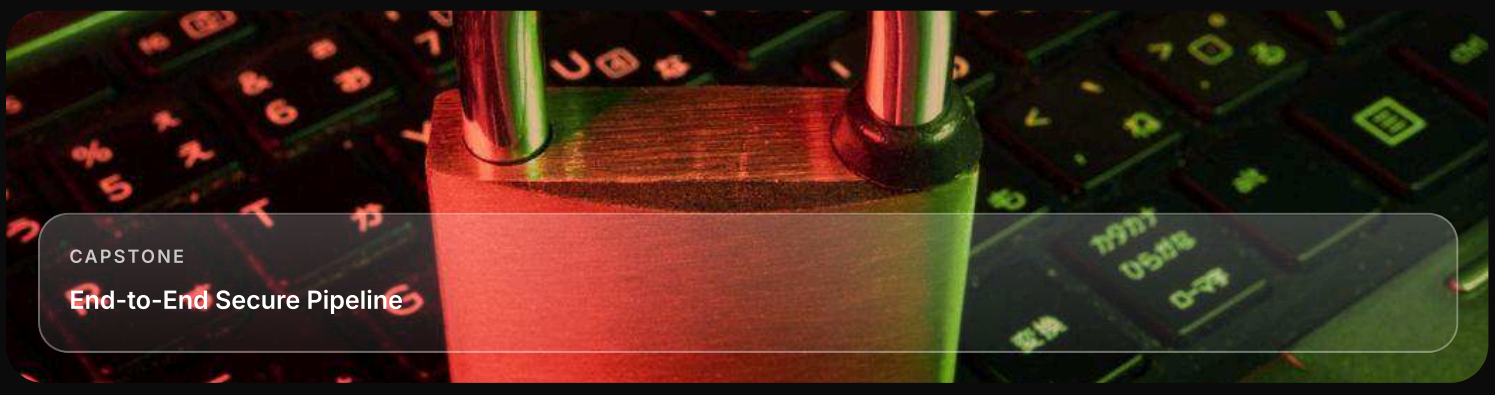
Monitoring and Security Culture

6 hours

Hands-on lab
Build a security metrics view for a sample delivery pipeline

TOPICS COVERED

- Pipeline observability
- Vulnerability metrics
- Feedback loops
- Developer enablement
- Security champions
- Continuous improvement



CAPSTONE

End-to-End Secure Pipeline



Git
Version control

GitHub
Code hosting & Actions CI

Docker
Containers & images

Kubernetes
Container orchestration

Jenkins
CI/CD pipelines

Frameworks & standards

- MITRE ATT&CK
- NIST CSF
- ISO 27001

FOCUS AREAS

Add SAST and dependency scanning to CI/CD	01
Scan containers and images	02
Apply policy as code	03
Build a security-first DevOps culture	04



LAB ACCESS

24×7 cloud labs for the length of the program

01

Secure CI/CD Pipeline

Build a CI/CD pipeline with integrated SAST, dependency and secret scanning, configuring sensible quality gates that do not block delivery.

02

Container Hardening

Scan and harden a sample container image, remediate findings and document a reusable secure-build checklist for development teams.

03

Policy as Code Guardrails

Implement policy-as-code rules that automatically flag or block insecure infrastructure and configuration changes in a sample repository.



Capstone project

End-to-End Secure Pipeline

Design and build a complete DevSecOps pipeline for a sample application, integrating code, dependency, container and configuration scanning with secrets management, policy as code and a security metrics view, then document how it supports secure, fast delivery.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-DSOE

Awarded on successful completion of the program assessments.

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



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

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

Phase 02

Apply

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

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

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

Learning path · Cloud & Application Security

Where this program fits.

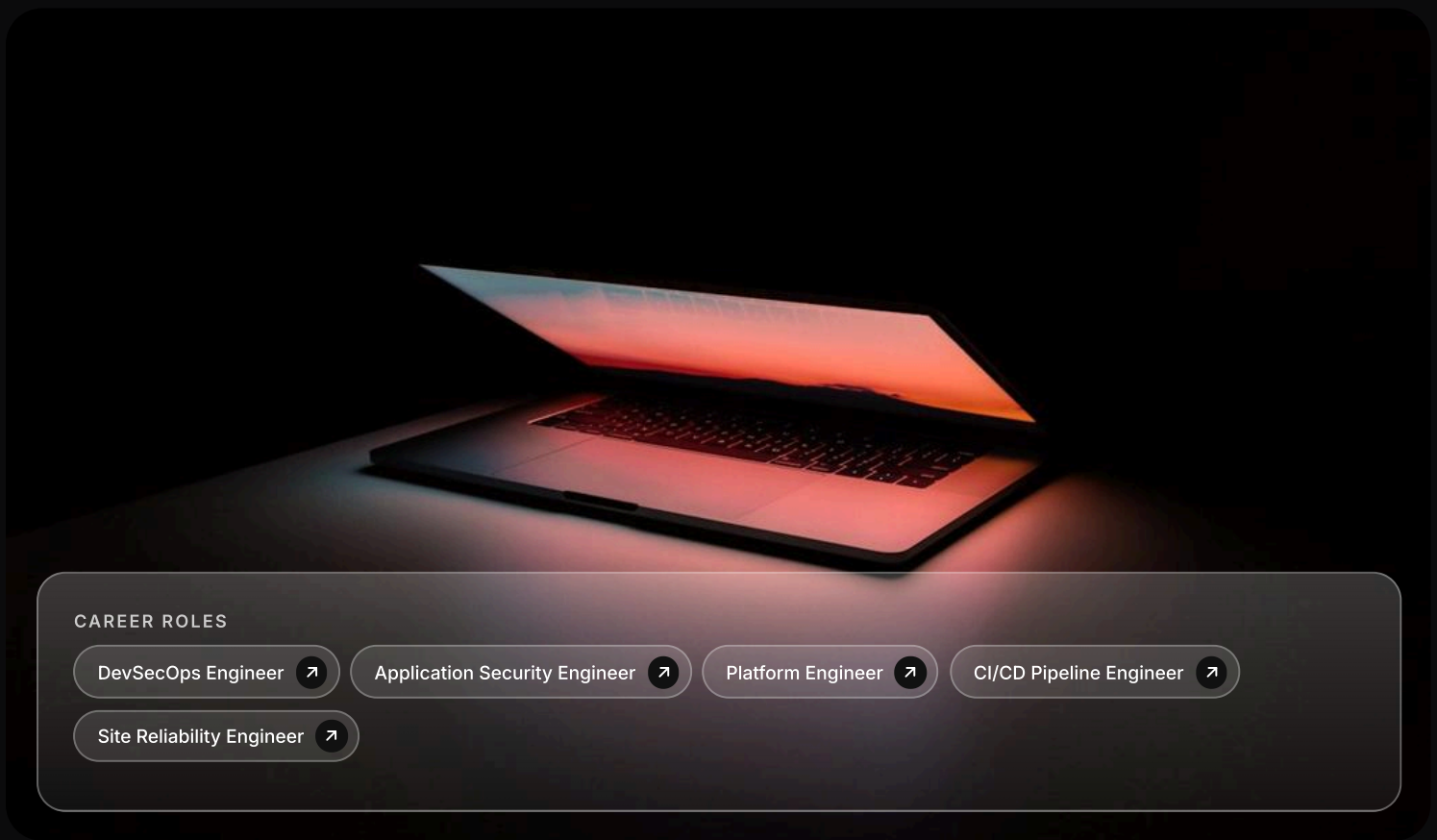
Beginner	Intermediate	Advanced	Expert
1 programs	You are here	3 programs	1 programs

Before this

Cloud Security Fundamentals	32 Hours

Up next

Application Security (SAST/DAST/IAST)	60 Hours
Cloud Penetration Testing	64 Hours
Kubernetes Security	40 Hours



CAREER ROLES

- DevSecOps Engineer
- Application Security Engineer
- Platform Engineer
- CI/CD Pipeline Engineer
- Site Reliability Engineer

Questions, answered.

Q01

Do I need prior experience to join?

Some development or DevOps familiarity helps. You should understand Git and basic CI/CD concepts, but you do not need to be an expert programmer to succeed.

Q02

How is the program delivered and scheduled?

The 48-hour program is instructor-led, delivered as live virtual sessions or in a blended format combining online and in-person classes in Surat. Weekday and weekend batch timings are confirmed at enrolment.

Q03

Will I receive a certificate?

Yes. The SAM-DSOE certificate is awarded after you attend the required sessions and successfully complete the program assessments, including practical exercises and the final capstone evaluation.

Q04

Will I get access to labs and tools?

You get guided lab environments and a list of open-source tools to install locally, so you can continue practising on your own systems after the course.

Q05

Is career support included?

Learners receive career guidance including resume and LinkedIn reviews, mock interviews and portfolio feedback. Outcomes depend on individual effort and market conditions, so the Academy does not guarantee jobs, placements or salaries.



Let's talk

START DEVSECOPS ESSENTIALS.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

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