Cloud & Application Security

Program Brochure · 2026

APPLICATION SECURITY

Find and fix flaws in code.

Advanced

60 Hours

SAM-APPSEC

Cybersecurity

Cloud & Application Security

8 programs in this track



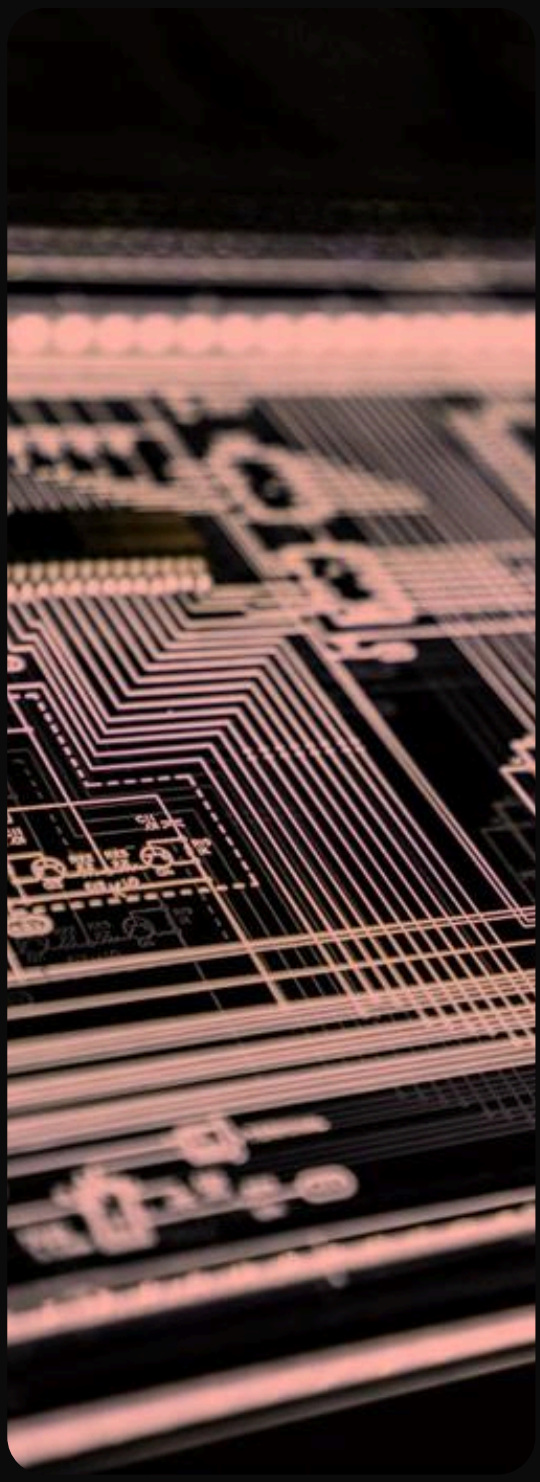
6

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	**Advanced**
Duration	**60 Hours**
Modules	**6**
Certificate	**SAM-APPSEC**

Program overview

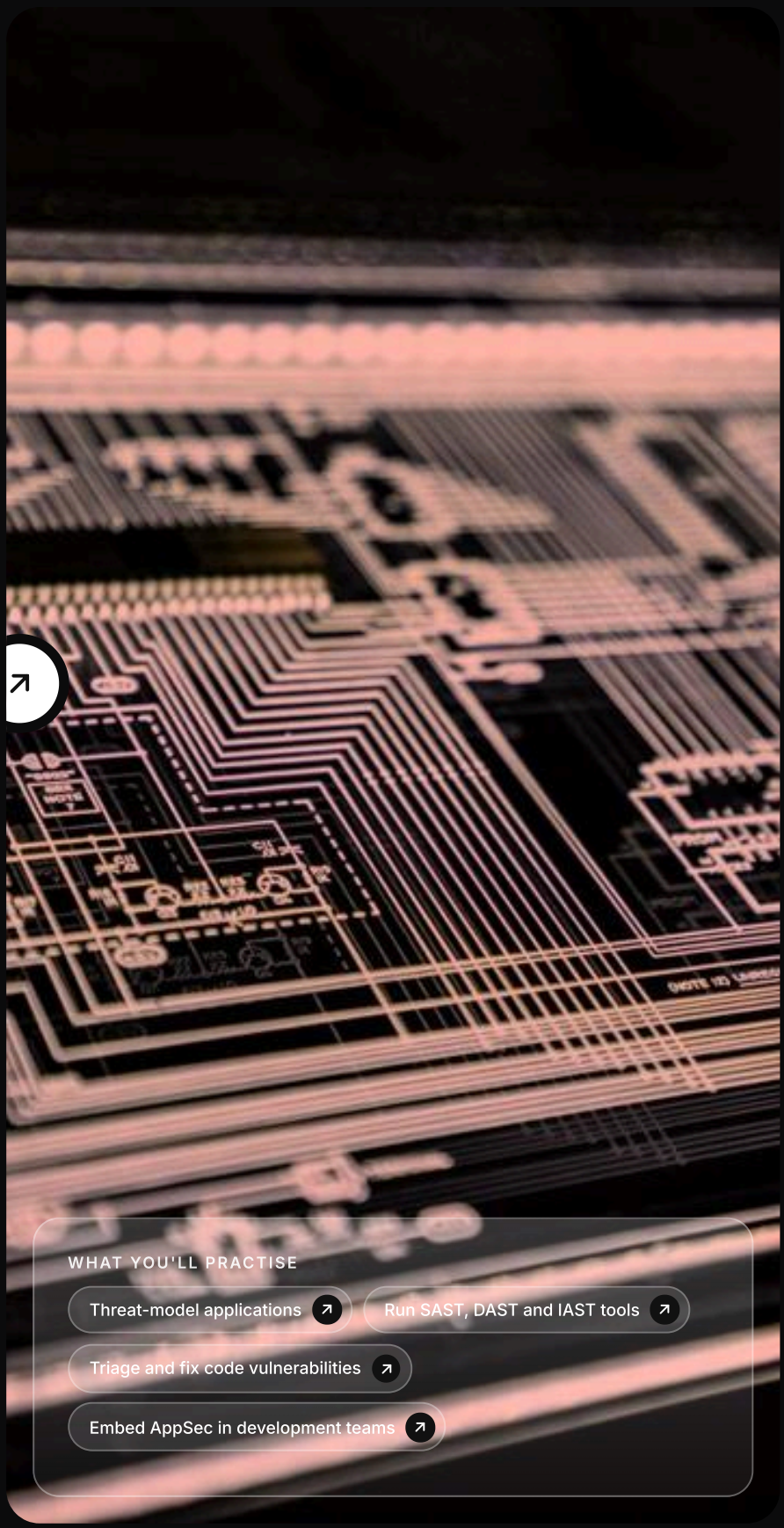
Find and fix flaws in code.

Secure software across the lifecycle with static, dynamic and interactive testing, threat modelling and secure coding.

Software flaws remain a leading cause of breaches, so organisations need specialists who can find and fix them across the lifecycle. This advanced program teaches secure software practices using static, dynamic and interactive testing alongside threat modelling and secure coding. You learn to triage and remediate code vulnerabilities and to embed application security into how development teams work.

DELIVERY

Instructor-led · Live virtual · Blended



LEVEL

Advanced

DURATION

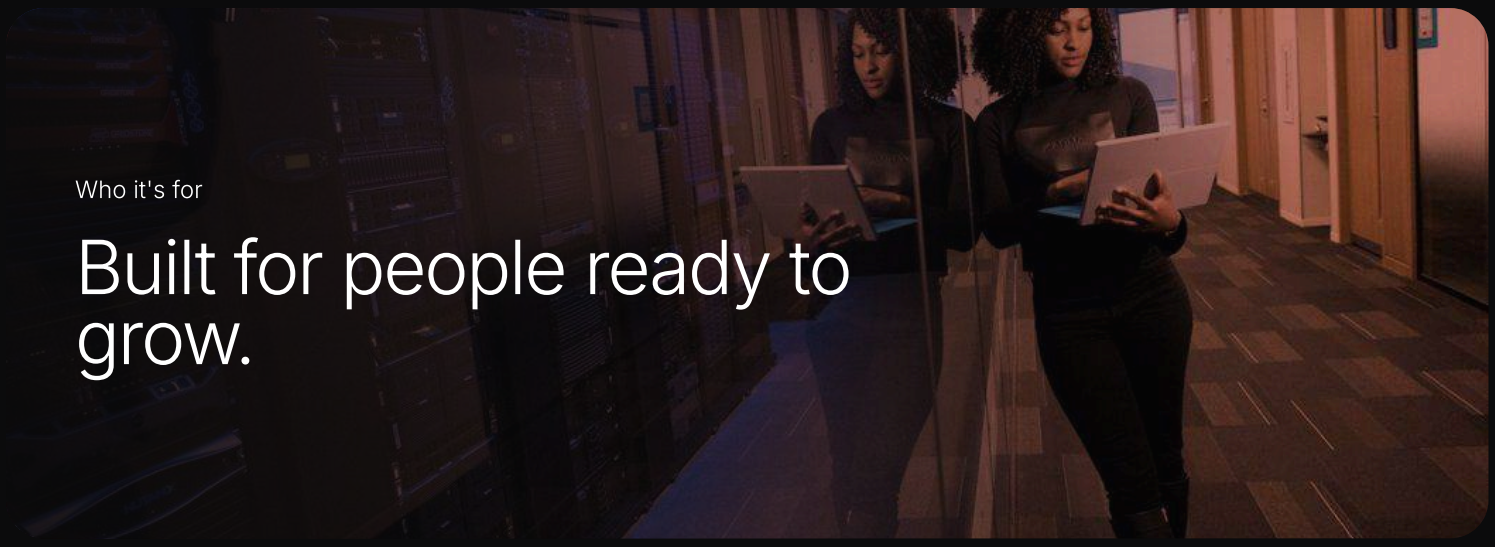
60 Hours

CERTIFICATION

SAM-APPSEC

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

- Understanding of web application vulnerabilities 01
- Basic programming or code-reading ability 02
- Familiarity with the software development lifecycle 03

ROLES THIS PREPARES YOU FOR

- Application Security Engineer ↗
- Product Security Engineer ↗
- Secure Code Reviewer ↗
- DevSecOps Engineer ↗
- Security Consultant (AppSec) ↗
- Software Engineer with Security Focus ↗

Learning outcomes

What you'll be able to do.



01	Threat-model applications systematically across the lifecycle
02	Run and tune SAST, DAST and IAST tools
03	Perform secure code reviews on real applications
04	Triage and prioritise code vulnerabilities by risk
05	Guide developers toward effective, verifiable remediation
06	Embed application security into everyday development teams

Program runway

Module by module.

6
modules · 60 hours

01	**AppSec Foundations and Threat Modelling** Secure SDLC, OWASP Top 10 review, Threat modelling methods	10 hrs
02	**Static Application Security Testing** SAST concepts, Tool configuration, Rule tuning	10 hrs
03	**Dynamic Application Security Testing** DAST concepts, Scanner configuration, Authenticated scanning	10 hrs
04	**Interactive Testing and Secure Coding** IAST concepts, Instrumentation basics, Combining testing methods	10 hrs
05	**Vulnerability Triage and Remediation** Risk-based prioritisation, CVSS scoring, Developer remediation guidance	10 hrs
06	**Embedding AppSec in Teams** Security gates in CI/CD, Security champions, Developer training	10 hrs
★	**Capstone · Full AppSec Assessment** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

AppSec Foundations and Threat Modelling

10 hours

Hands-on lab
Threat-model a sample application and document key abuse cases

TOPICS COVERED

- Secure SDLC
- OWASP Top 10 review
- Threat modelling methods
- Data flow diagrams
- Abuse cases
- Security requirements

OWASP

Module 02

Static Application Security Testing

10 hours

Hands-on lab
Run a SAST scan, triage results and tune rules to cut false positives

TOPICS COVERED

- SAST concepts
- Tool configuration
- Rule tuning
- False positive triage
- Code review integration
- Pipeline integration

Module 03

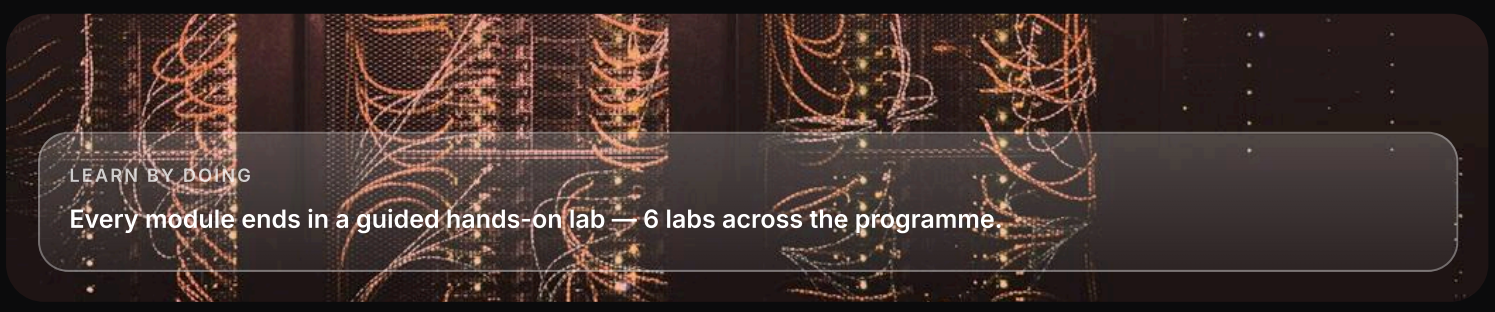
Dynamic Application Security Testing

10 hours

Hands-on lab
Configure an authenticated DAST scan and validate the findings

TOPICS COVERED

- DAST concepts
- Scanner configuration
- Authenticated scanning
- API testing
- Findings validation
- Coverage limits



LEARN BY DOING

Every module ends in a guided hands-on lab — 6 labs across the programme.

Syllabus, continued.

Modules 04–06

Module 04

Interactive Testing and Secure Coding

10 hours

Hands-on lab
Compare SAST, DAST and IAST results on the same sample application

TOPICS COVERED

- IAST concepts
- Instrumentation basics
- Combining testing methods
- Secure coding patterns
- Input validation and output encoding
- Language-specific pitfalls

Module 05

Vulnerability Triage and Remediation

10 hours

Hands-on lab
Triage a mixed findings set and write developer remediation guidance

TOPICS COVERED

- Risk-based prioritisation
- CVSS scoring
- Developer remediation guidance
- Fix verification
- Dependency and SCA
- Metrics and tracking

Module 06

Embedding AppSec in Teams

10 hours

Hands-on lab
Design an AppSec programme and gate strategy for a sample team

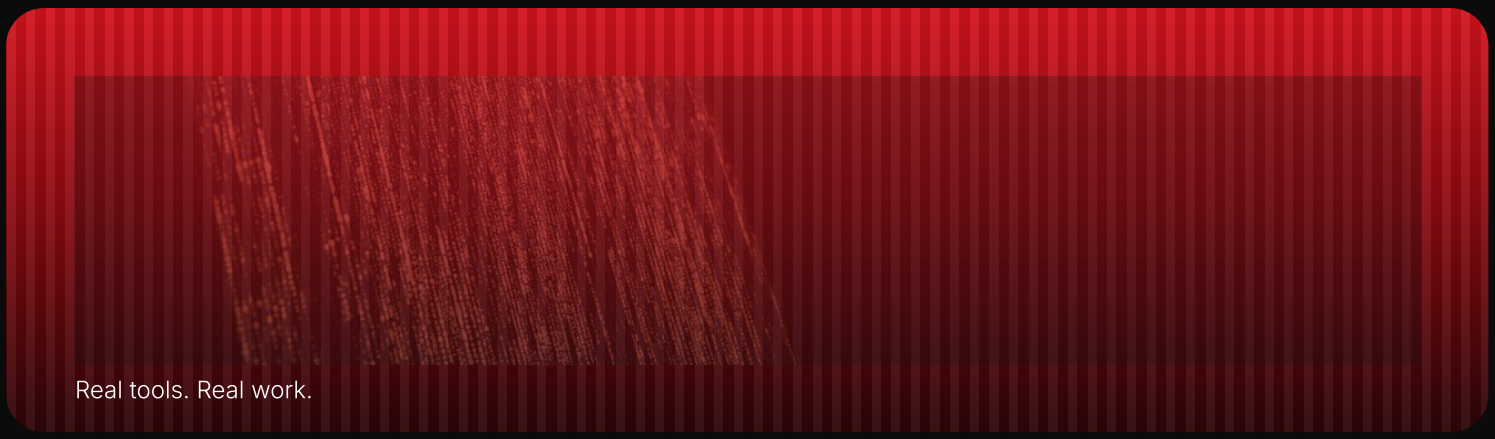
TOPICS COVERED

- Security gates in CI/CD
- Security champions
- Developer training
- Programme metrics
- Maturity models
- Continuous improvement



CAPSTONE

Full AppSec Assessment



OWASP
Top 10 & testing standards

Burp Suite
Web app security testing

GitHub
Code hosting & Actions CI

Python
Automation & scripting

Frameworks & standards

OWASP

FOCUS AREAS

Threat-model applications	01
Run SAST, DAST and IAST tools	02
Triage and fix code vulnerabilities	03
Embed AppSec in development teams	04



LAB ACCESS

24×7 cloud labs for the length of the program

01

Application Threat Model

Produce a complete threat model for a sample application, documenting data flows, abuse cases and prioritised security requirements.

02

Multi-Tool Testing Report

Run SAST, DAST and IAST against a sample application, compare coverage and consolidate the findings into a single prioritised report.

03

Remediation Guidance Pack

Triage a set of vulnerabilities and write clear, developer-friendly remediation guidance with verification steps for each issue.



Capstone project

Full AppSec Assessment

Deliver an end-to-end application security engagement on a sample app, from threat model through combined SAST, DAST and IAST testing to a triaged, prioritised findings report with remediation guidance and a plan to embed AppSec in the team.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-APPSEC

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	3 programs	You are here	1 programs

Before this

AWS Security Specialty Prep	56 Hours
Azure Security Engineer (AZ-500) Prep	56 Hours
DevSecOps Essentials	48 Hours

Up next

Cloud Security Architecture	72 Hours



CAREER ROLES

- Application Security Engineer
- Product Security Engineer
- Secure Code Reviewer
- DevSecOps Engineer
- Security Consultant (AppSec)

Questions, answered.

Q01

Do I need prior experience to join?

Yes, some background helps. You should understand common web vulnerabilities and be able to read code, as this advanced course goes deep into testing and remediation.

Q02

How is the program delivered and scheduled?

The 60-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-APPSEC 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 APPLICATION SECURITY.

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