Cloud & Application Security

Program Brochure · 2026

CLOUD SECURITY ARCHITECTURE

Design secure cloud at scale.

Expert

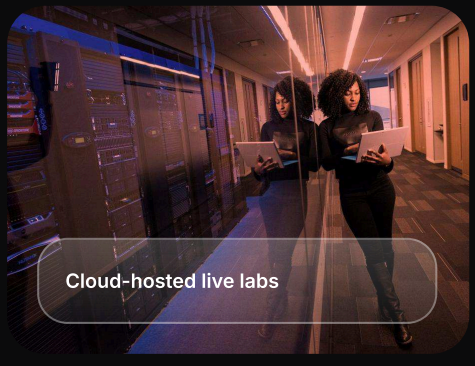
72 Hours

SAM-CSA

Cybersecurity

Cloud & Application Security

8 programs in this track



7

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 10

Projects & capstone 11

Certification & method 12

Learning path 13

FAQs 14



AT A GLANCE

Level	**Expert**
Duration	**72 Hours**
Modules	**7**
Certificate	**SAM-CSA**

Program overview

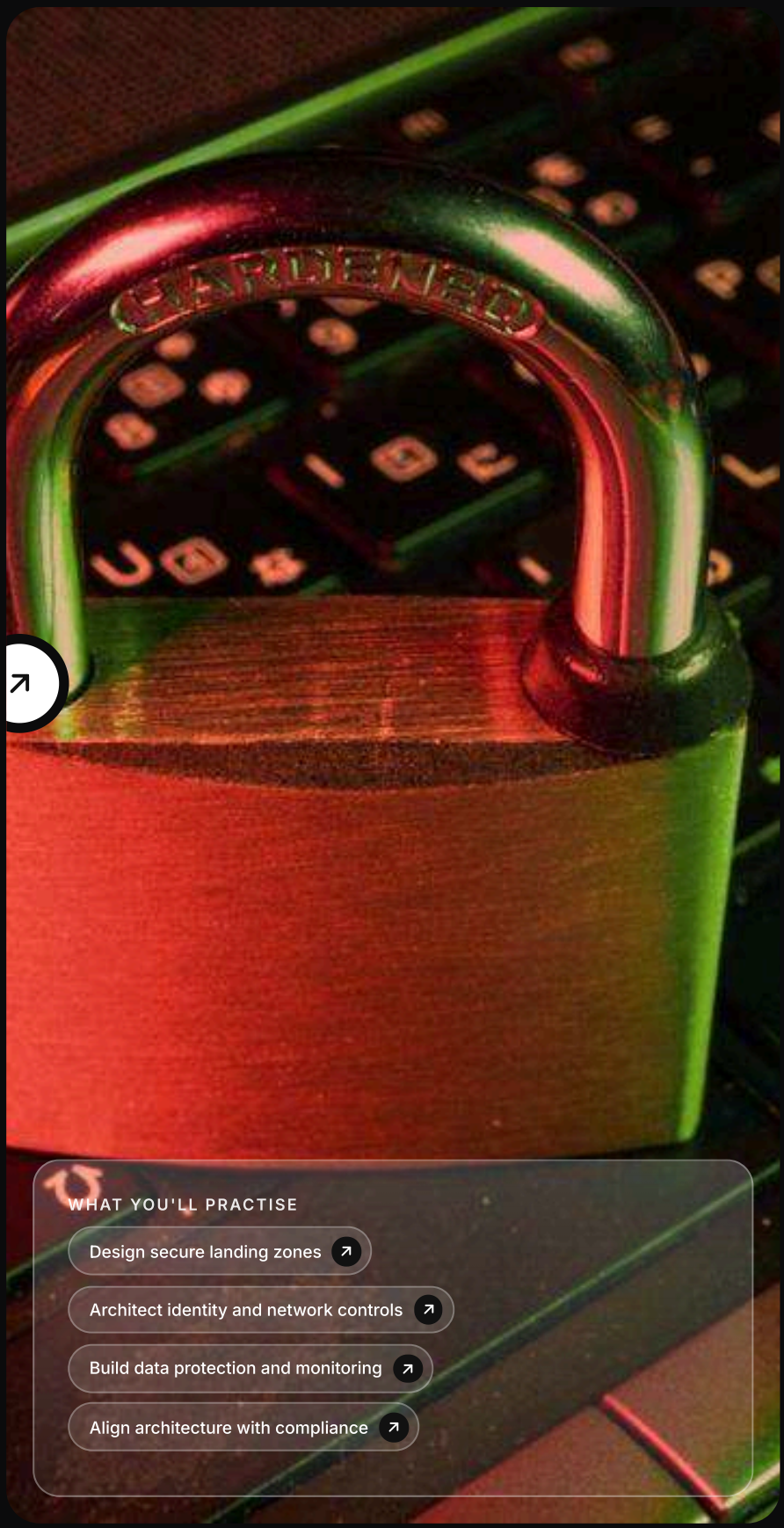
Design secure cloud at scale.

Architect secure, compliant multi-account and multi-cloud environments with identity, network, data and monitoring controls.

Large organisations run complex multi-account and multi-cloud estates that must be secure and compliant by design. This expert program teaches you to architect secure landing zones and identity, network, data and monitoring controls that scale. You finish able to design cloud architectures that align with compliance requirements and hold up under real operational and audit pressure.

DELIVERY

Instructor-led · Live virtual · Blended

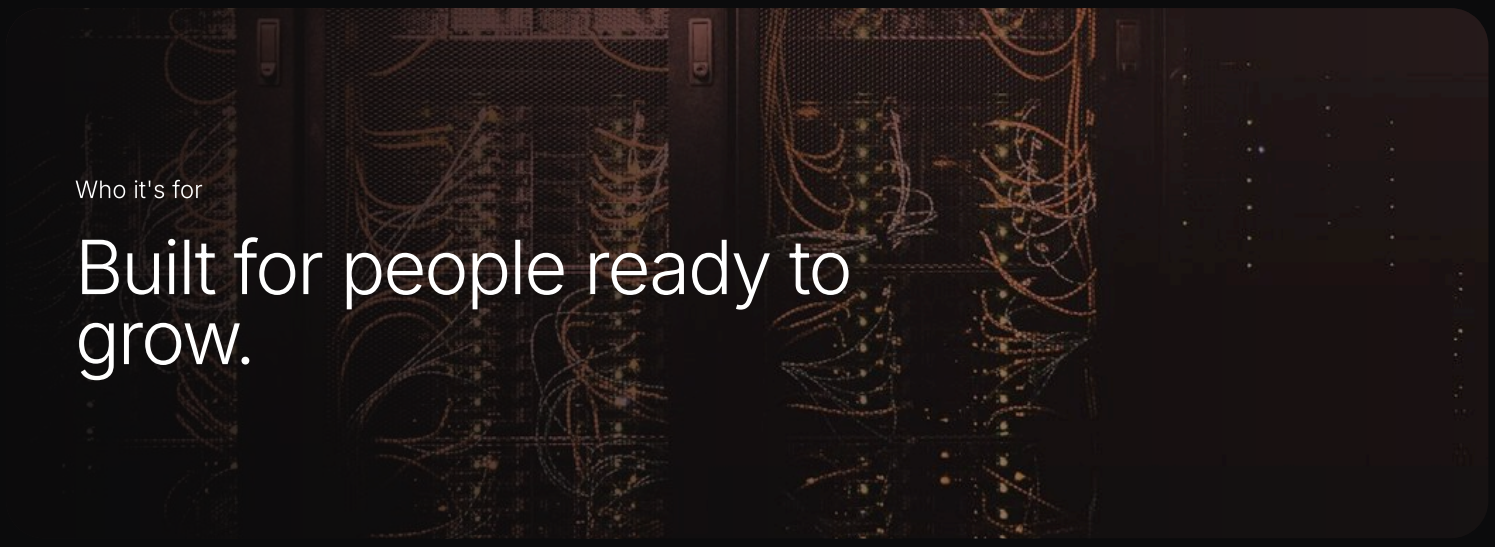


LEVEL
Expert

DURATION
72 Hours

CERTIFICATION
SAM-CSA

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

Strong cloud security fundamentals	01
Hands-on experience with one or more cloud providers	02
Understanding of networking and identity concepts	03

ROLES THIS PREPARES YOU FOR

- Cloud Security Architect ↗
- Security Solutions Architect ↗
- Principal Cloud Engineer ↗
- Enterprise Security Architect ↗
- Cloud Governance Lead ↗
- Senior Cloud Security Engineer ↗

Learning outcomes

What you'll be able to do.



01 Design secure multi-account and multi-cloud landing zones

02 Architect scalable identity and network security controls

03 Build data protection and encryption strategies at scale

04 Design monitoring and threat detection across the estate

05 Align cloud architecture with relevant compliance requirements

06 Document and defend architecture decisions under review

Program runway

Module by module.

7
modules · 72 hours

01	**Security Architecture Foundations** Architecture principles, Reference architectures, Threat modelling at scale	10 hrs
02	**Landing Zones and Account Structure** Multi-account design, Landing zone patterns, Organisational guardrails	12 hrs
03	**Identity Architecture** Enterprise identity design, Federation and SSO, Least privilege at scale	10 hrs
04	**Network Architecture** Hub-and-spoke networks, Segmentation strategy, Secure connectivity	10 hrs
05	**Data Protection Architecture** Encryption strategy, Key management design, Data classification	10 hrs
06	**Monitoring and Detection Design** Centralised monitoring, Detection architecture, Security data lakes	10 hrs
07	**Compliance and Governance** Mapping controls to compliance, Policy as code at scale, Audit readiness	10 hrs
★	**Capstone · Enterprise Cloud Security Blueprint** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Security Architecture Foundations

10 hours

Hands-on lab
Produce an architecture decision record for a sample platform choice

TOPICS COVERED

- Architecture principles
- Reference architectures
- Threat modelling at scale
- Well-Architected frameworks
- Trade-off analysis
- Decision records

Module 02

Landing Zones and Account Structure

12 hours

Hands-on lab
Design a secure multi-account landing zone for a sample enterprise

TOPICS COVERED

- Multi-account design
- Landing zone patterns
- Organisational guardrails
- Centralised logging
- Baseline controls
- Scalable account vending

Module 03

Identity Architecture

10 hours

Hands-on lab
Architect a scalable identity and access model across accounts

TOPICS COVERED

- Enterprise identity design
- Federation and SSO
- Least privilege at scale
- Role and permission models
- Workload identity
- Access governance

LEARN BY DOING

Every module ends in a guided hands-on lab — 7 labs across the programme.

Syllabus, continued.

Modules 04–05

Module 04

Network Architecture

10 hours

Hands-on lab
Design a segmented hub-and-spoke network with controlled egress

TOPICS COVERED

- Hub-and-spoke networks
- Segmentation strategy
- Secure connectivity
- Edge and ingress design
- Private service access
- Traffic inspection

Module 05

Data Protection Architecture

10 hours

Hands-on lab
Design an enterprise key management and data protection strategy

TOPICS COVERED

- Encryption strategy
- Key management design
- Data classification
- Secrets architecture
- Backup and resilience
- Data residency



LEARN BY DOING

Every module ends in a guided hands-on lab — 7 labs across the programme.

Syllabus, continued.

Modules 06–07

Module 06

Monitoring and Detection Design

10 hours

Hands-on lab
Architect a centralised monitoring and threat detection pipeline across accounts

TOPICS COVERED

- Centralised monitoring
- Detection architecture
- Security data lakes
- Alerting strategy
- Automated response
- Observability at scale

Module 07

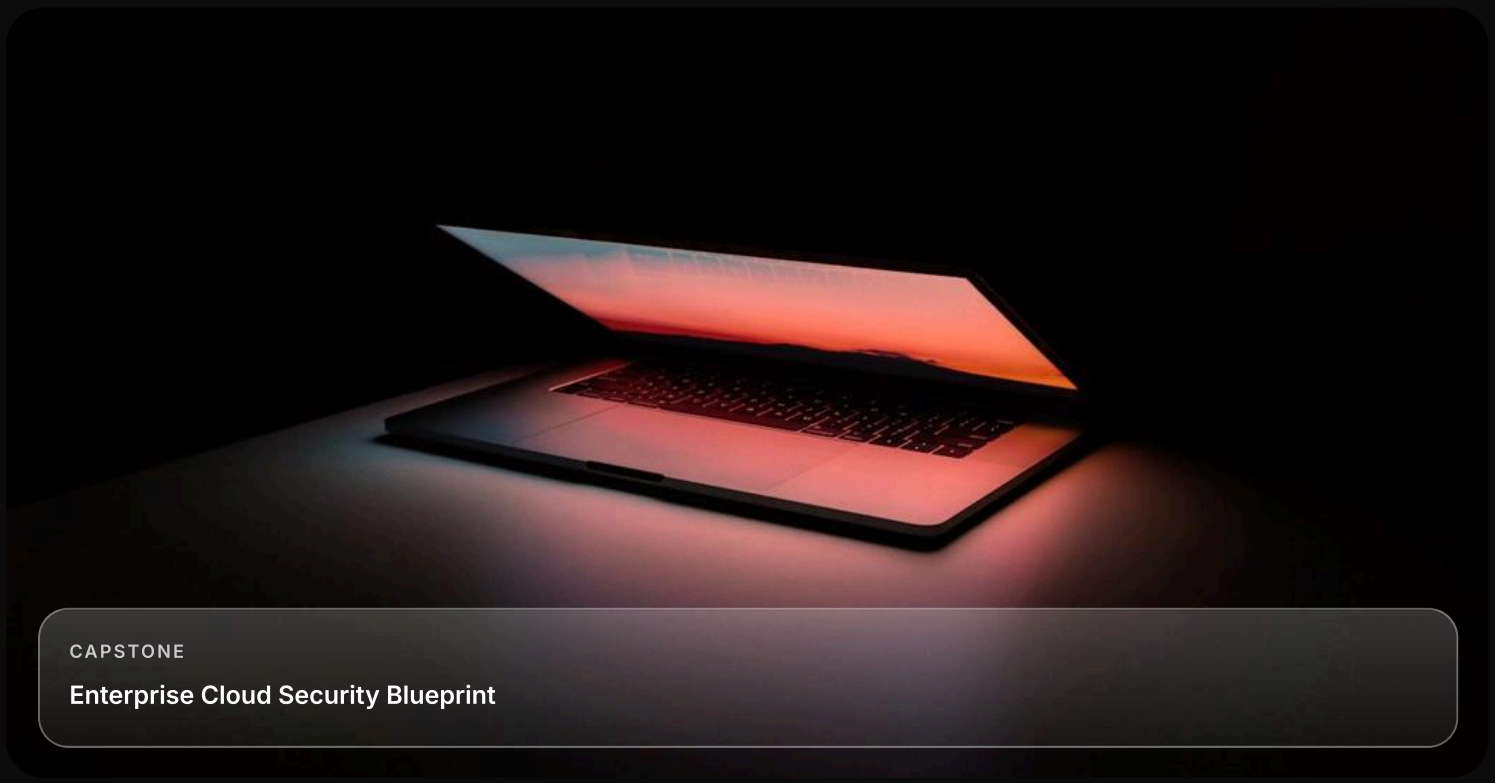
Compliance and Governance

10 hours

Hands-on lab
Map a reference architecture to a chosen compliance framework

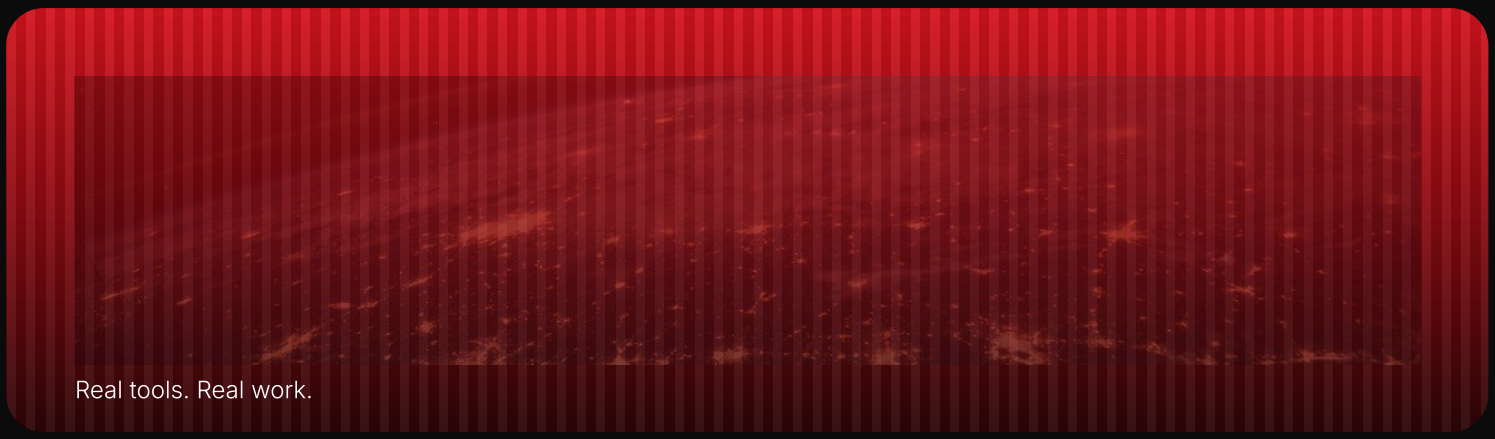
TOPICS COVERED

- Mapping controls to compliance
- Policy as code at scale
- Audit readiness
- Risk and exceptions
- Architecture governance
- Continuous assurance



CAPSTONE

Enterprise Cloud Security Blueprint



AWS
Cloud platform

Microsoft Azure
Cloud platform

Google Cloud
Cloud platform

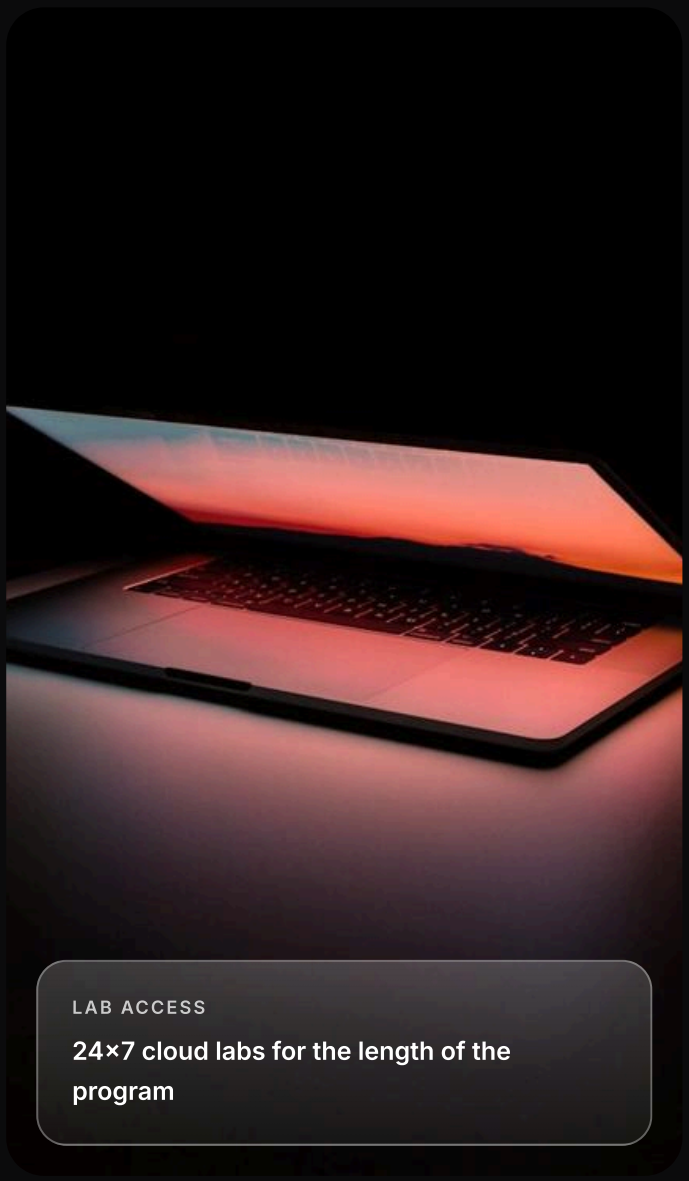
Terraform
Infrastructure as code

Frameworks & standards

- MITRE ATT&CK
- NIST CSF
- ISO 27001

FOCUS AREAS

Design secure landing zones	01
Architect identity and network controls	02
Build data protection and monitoring	03
Align architecture with compliance	04



LAB ACCESS

24×7 cloud labs for the length of the program

01

Secure Landing Zone

Design a secure multi-account landing zone for a sample enterprise, with guardrails, centralised logging and baseline controls, documented as reference architecture.

02

Identity and Network Design

Architect scalable identity and segmented network controls for a multi-account estate, justifying each decision against security and operational needs.

03

Compliance-Aligned Architecture

Map a complete cloud architecture to a chosen compliance framework, documenting how each control requirement is satisfied by design.



Capstone project

Enterprise Cloud Security Blueprint

Design a complete, compliance-aligned cloud security architecture for a sample enterprise, covering landing zones, identity, network, data protection and monitoring, captured as reference diagrams and decision records, then defend it in a simulated architecture review.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-CSA

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.

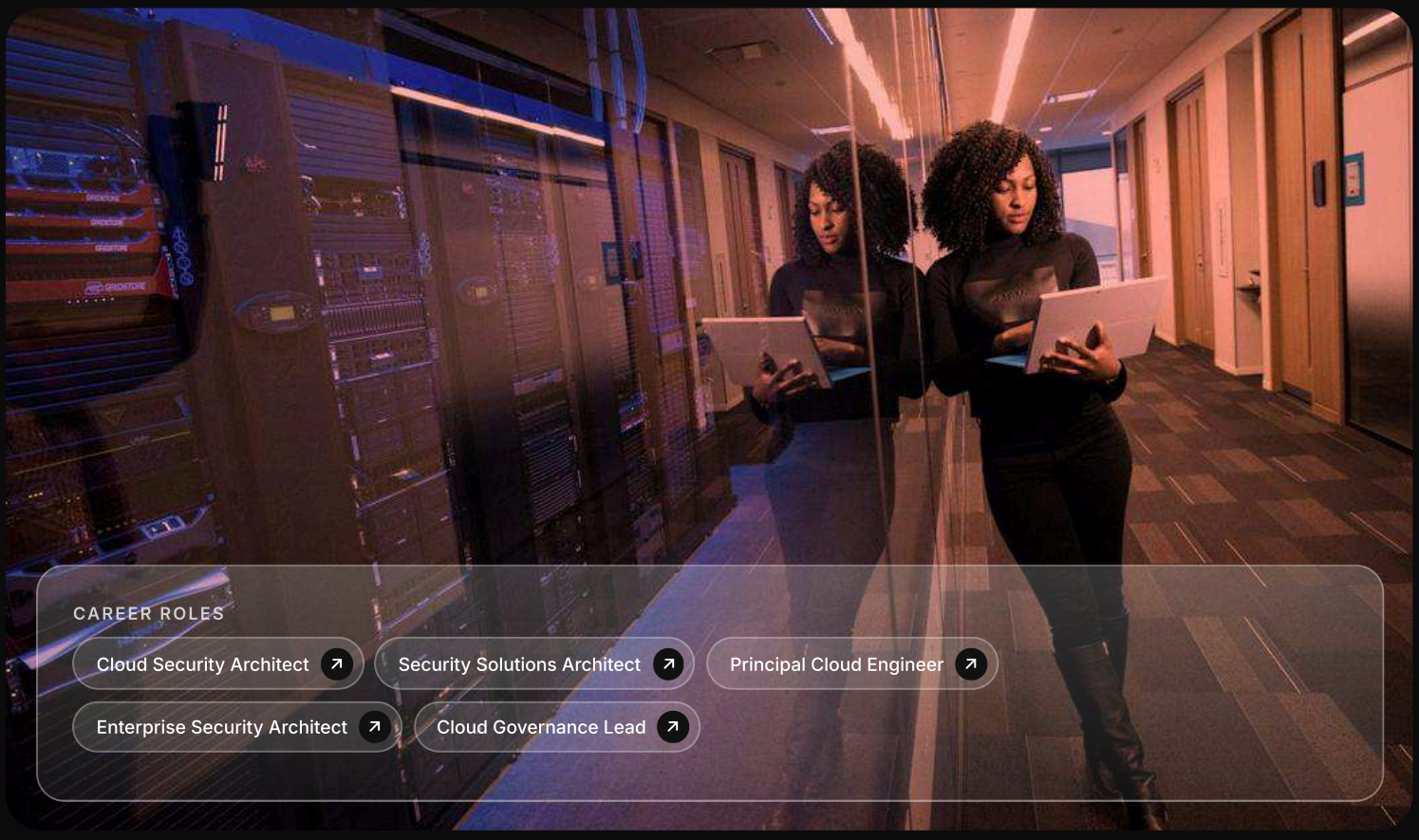
Beginner	Intermediate	Advanced	Expert
1 programs	3 programs	3 programs	You are here

Before this

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

Up next

The top of this pathway — explore related tracks.



Questions, answered.

Q01

Do I need prior experience to join?

Yes. This is an expert-level course. You should have strong cloud security fundamentals and hands-on experience with at least one major provider before enrolling, as we focus on large-scale architecture design, trade-offs and decision records rather than introductory concepts.

Q02

How is the program delivered and scheduled?

The 72-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-CSA 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?

All hands-on work runs in isolated sandbox cloud accounts and lab environments provided for the course, with setup guides for free-tier and local alternatives you can keep using after the program.

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 CLOUD SECURITY ARCHITECTURE.

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