Cloud & Application Security

Program Brochure · 2026

CLOUD PENETRATION TESTING

Attack the cloud, ethically.

Advanced

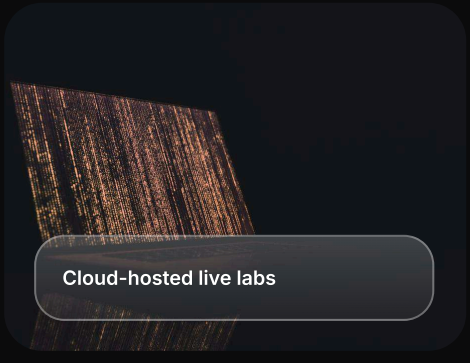
64 Hours

SAM-CLDPT

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	**64 Hours**
Modules	**6**
Certificate	**SAM-CLDPT**

Program overview

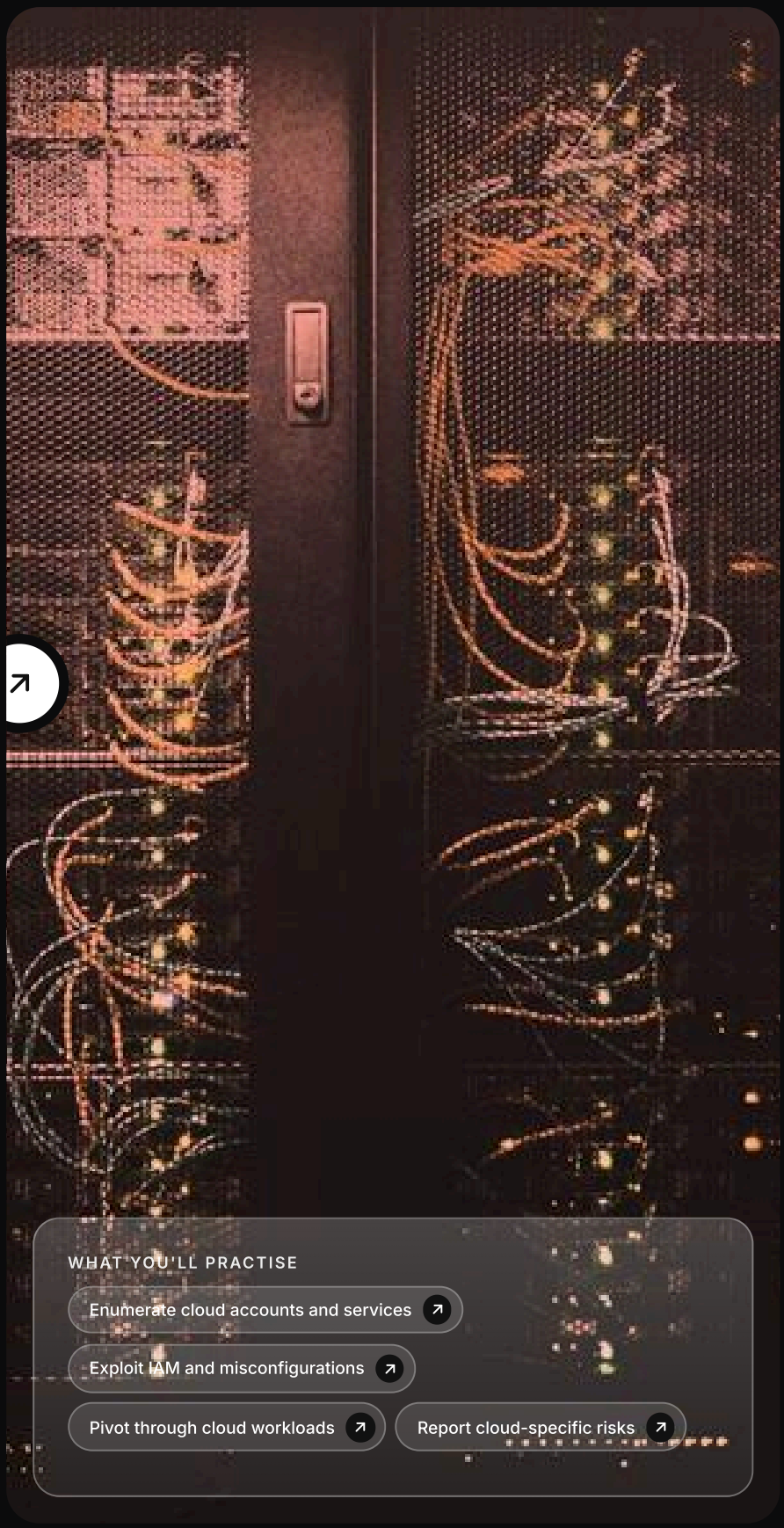
Attack the cloud, ethically.

Test AWS, Azure and GCP environments for misconfigurations, identity weaknesses and exploitable cloud services.

Cloud environments fail in different ways from traditional networks, so organisations need testers who understand identity, services and misconfiguration at depth. This advanced program teaches you to assess AWS, Azure and GCP environments for weaknesses, enumerate services, exploit identity flaws in authorised labs and report cloud-specific risks clearly, always within scope and with provider rules in mind.

DELIVERY

Instructor-led · Live virtual · Blended

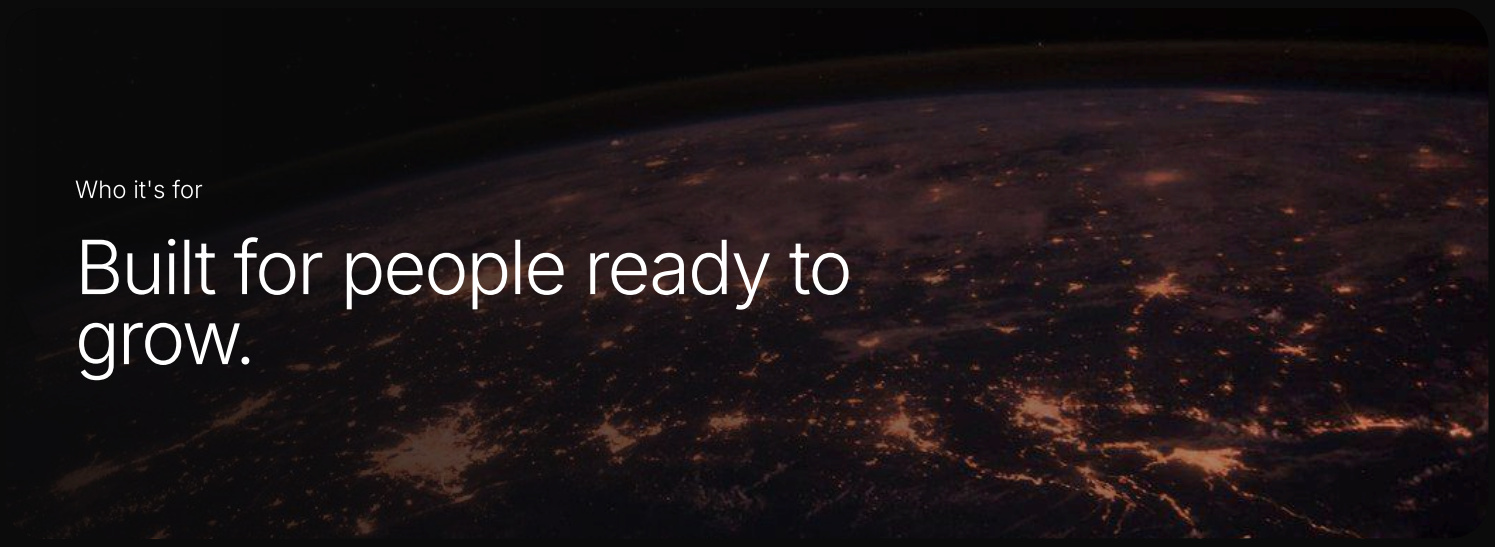


LEVEL
Advanced

DURATION
64 Hours

CERTIFICATION
SAM-CLDPT

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

- Solid penetration testing fundamentals 01
- Working knowledge of at least one cloud provider 02
- Comfort with scripting and the command line 03

ROLES THIS PREPARES YOU FOR

- Cloud Penetration Tester ↗
- Offensive Security Engineer ↗
- Cloud Security Consultant ↗
- Red Team Operator ↗
- Security Assessor ↗
- Cloud Security Engineer ↗

Learning outcomes

What you'll be able to do.



01	Enumerate cloud accounts, identities and exposed services
02	Identify and assess IAM misconfigurations and escalation paths
03	Exploit insecure cloud services in authorised lab environments
04	Pivot safely and in scope through cloud workloads
05	Map findings to provider security best practices
06	Report cloud-specific risks with clear remediation guidance

Program runway

Module by module.

6
modules · 64 hours

01	**Cloud Pentest Foundations** Cloud attack surface, Provider rules of engagement, Scoping cloud tests	8 hrs
02	**Identity and Access Exploitation** IAM enumeration, Privilege escalation paths, Role assumption issues	12 hrs
03	**Service and Storage Misconfigurations** Storage exposure, Serverless function risks, Metadata service abuse	12 hrs
04	**Workload and Network Pivoting** Compute workload testing, Container and cluster exposure, Network path analysis	12 hrs
05	**Multi-Cloud Testing** AWS-specific issues, Azure-specific issues, GCP-specific issues	12 hrs
06	**Reporting and Remediation** Evidence capture, Risk rating cloud findings, Clear remediation mapping	8 hrs
★	**Capstone · Full Cloud Assessment Engagement** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Cloud Pentest Foundations

8 hours

Hands-on lab
Scope an authorised cloud test and confirm provider testing rules

TOPICS COVERED

- Cloud attack surface
- Provider rules of engagement
- Scoping cloud tests
- Shared responsibility impact
- Methodology overview
- Tooling setup

Module 02

Identity and Access Exploitation

12 hours

Hands-on lab
Map and assess privilege escalation paths in a vulnerable lab account

TOPICS COVERED

- IAM enumeration
- Privilege escalation paths
- Role assumption issues
- Credential exposure
- Policy misconfigurations
- Access key hygiene

Module 03

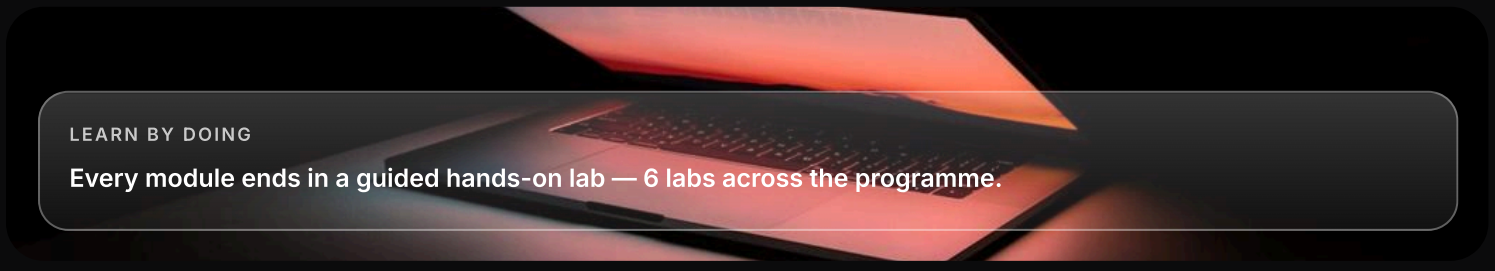
Service and Storage Misconfigurations

12 hours

Hands-on lab
Discover and document exposed storage and services in a lab tenant

TOPICS COVERED

- Storage exposure
- Serverless function risks
- Metadata service abuse
- Database exposure
- Logging gaps
- Exposed management surfaces



LEARN BY DOING

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

Syllabus, continued.

Modules 04–06

Module 04

Workload and Network Pivoting

12 hours

Hands-on lab
Demonstrate controlled lateral movement across a lab cloud workload

TOPICS COVERED

- Compute workload testing
- Container and cluster exposure
- Network path analysis
- Lateral movement concepts
- Hybrid connectivity risks
- Containment awareness

Module 05

Multi-Cloud Testing

12 hours

Hands-on lab
Assess a multi-cloud lab scenario and compare provider-specific risks

TOPICS COVERED

- AWS-specific issues
- Azure-specific issues
- GCP-specific issues
- Cross-account trust
- Tooling comparison
- Provider best practices

AWS Google Cloud

Module 06

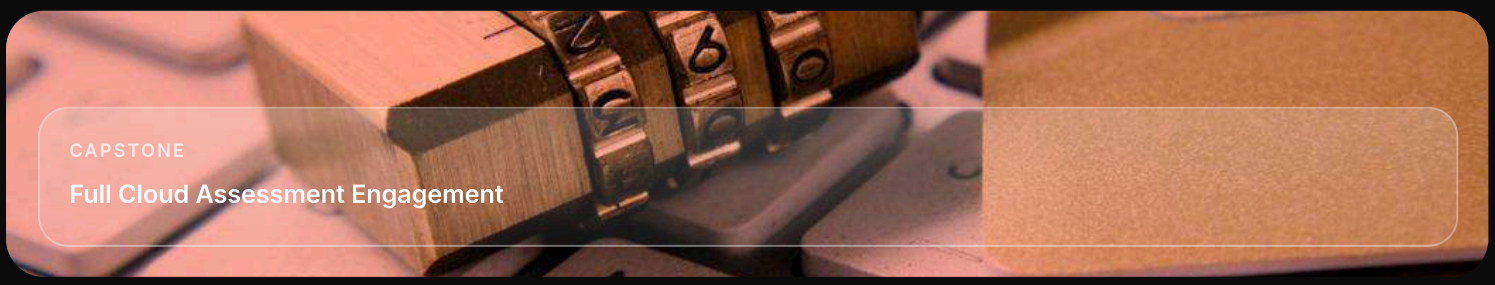
Reporting and Remediation

8 hours

Hands-on lab
Write a cloud pentest report mapping findings to provider guidance

TOPICS COVERED

- Evidence capture
- Risk rating cloud findings
- Clear remediation mapping
- Executive summaries
- Retesting and validation
- Responsible disclosure



CAPSTONE

Full Cloud Assessment Engagement



AWS
Cloud platform

Microsoft Azure
Cloud platform

Google Cloud
Cloud platform

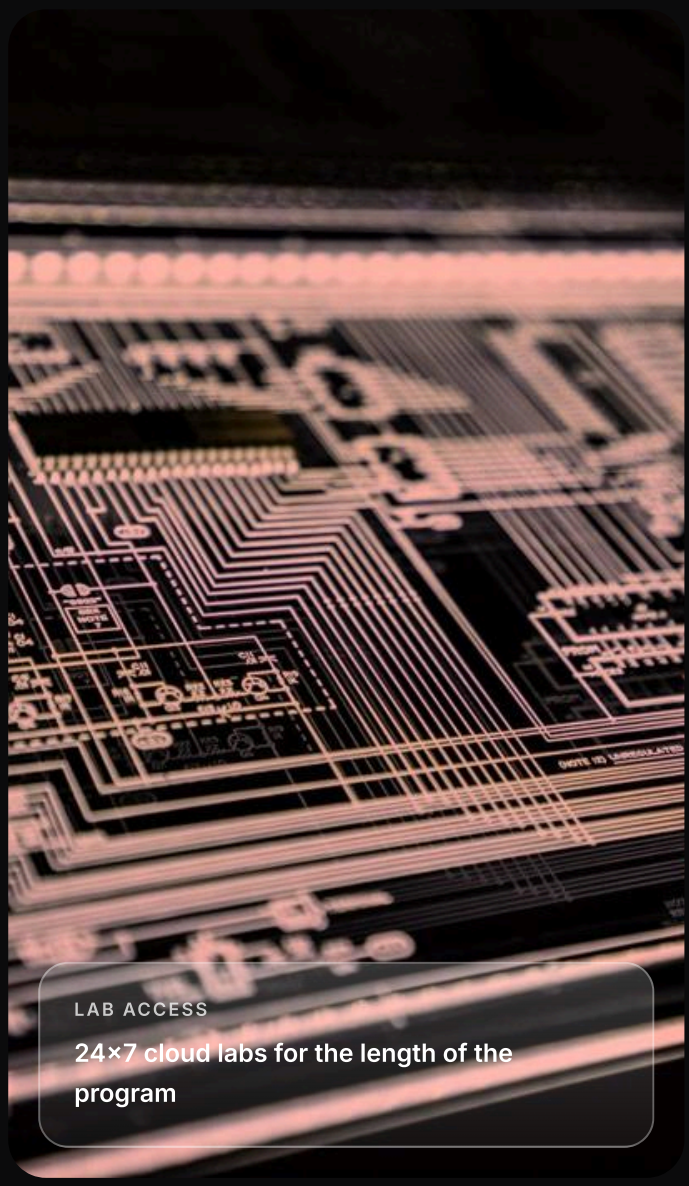
Kali Linux
Security testing distribution

Frameworks & standards

- MITRE ATT&CK
- NIST CSF
- ISO 27001

FOCUS AREAS

Enumerate cloud accounts and services	01
Exploit IAM and misconfigurations	02
Pivot through cloud workloads	03
Report cloud-specific risks	04



01

IAM Weakness Assessment

Assess a vulnerable lab cloud account for identity misconfigurations and privilege escalation paths, documenting each with clear remediation advice.

02

Misconfiguration Report

Discover exposed storage, services and metadata risks in a lab tenant and compile a prioritised, provider-mapped findings report.

03

Multi-Cloud Test Summary

Assess a multi-cloud lab scenario and produce a consolidated report comparing the key risks and fixes across each provider.



Capstone project

Full Cloud Assessment Engagement

Conduct an end-to-end authorised cloud penetration test across a multi-cloud lab, from scoping and identity analysis to service misconfigurations and controlled pivoting, then deliver a professional report mapping every finding to provider best practices and remediations.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-CLDPT

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.

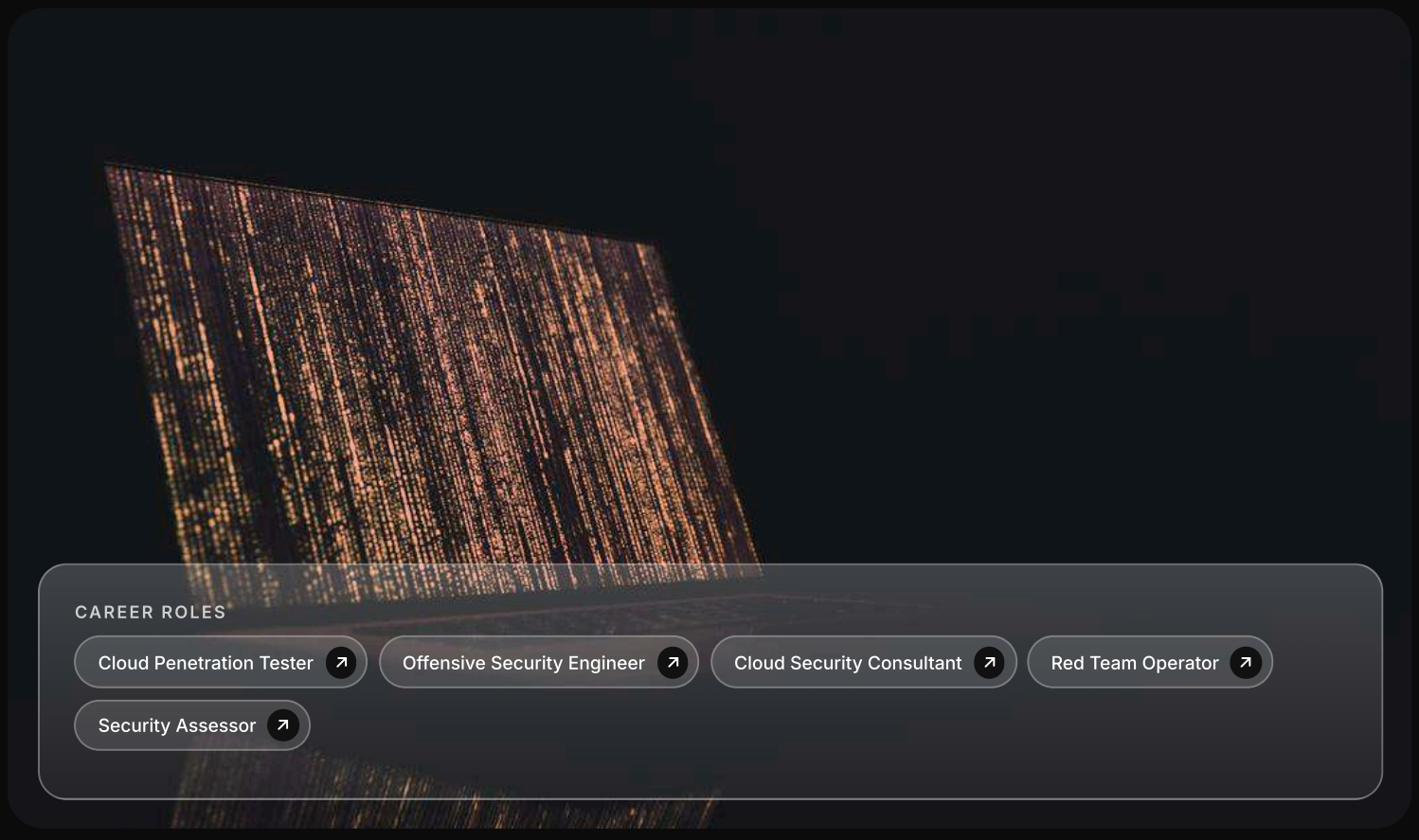
Beginner	Intermediate	Advanced	Expert
1 programs	3 programs	You are here	1 programs

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

- Cloud Penetration Tester
- Offensive Security Engineer
- Cloud Security Consultant
- Red Team Operator
- Security Assessor

Questions, answered.

Q01

Do I need prior experience to join?

Yes. This is an advanced course that assumes you already have solid penetration testing fundamentals and working knowledge of at least one major cloud provider, since we move quickly into identity exploitation, misconfigurations and pivoting within authorised cloud lab environments.

Q02

How is the program delivered and scheduled?

The 64-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-CLDPT 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 PENETRATION TESTING.

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