✦ CLOUD COMPUTING · EXPERT

Cloud Security

Defend workloads across clouds.





72	8	SAM-CLDSEC
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	Expert
Duration	72 Hours
Modules	8
Certificate	SAM-CLDSEC

✦ PROGRAM OVERVIEW

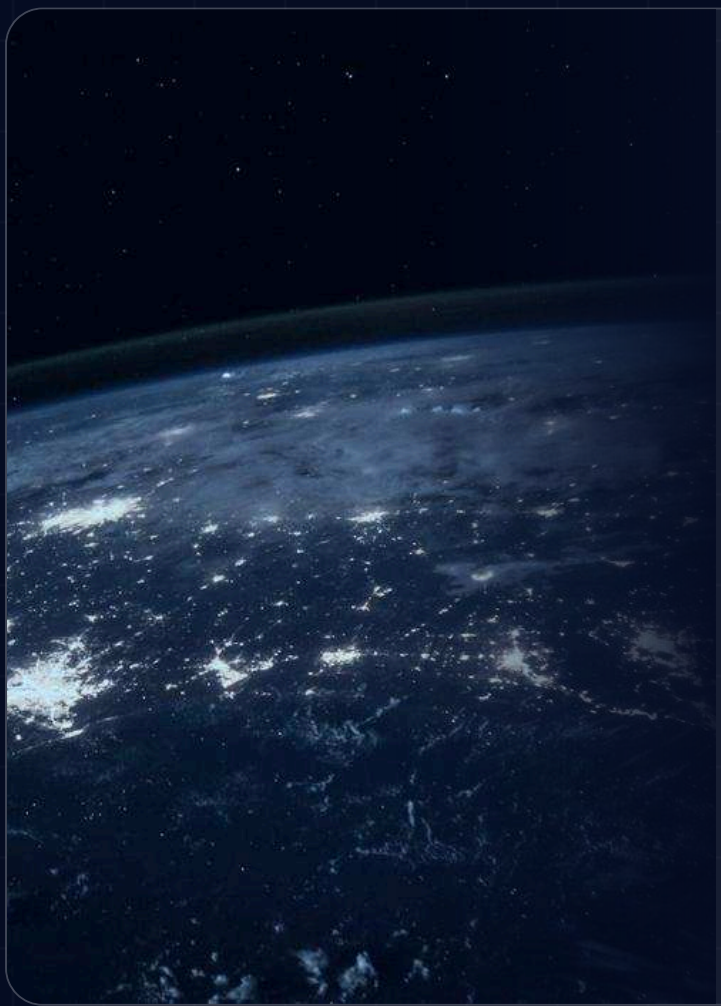
Defend workloads across clouds.



Expert cloud security across AWS and Azure — identity, network, data, detection and response.

Most cloud breaches stem from misconfigurations, excessive permissions and gaps in monitoring rather than provider failures. This expert program builds deep, hands-on security skills across AWS and Azure: identity, network and data protection, posture management, threat detection, incident response and security automation, mapped to frameworks such as CIS Benchmarks and NIST.

LEVEL	DURATION	CERTIFICATION	DELIVERY
Expert	72 Hours	SAM-CLDSEC	Instructor-led · Live virtual · Blended



✦ WHAT YOU'LL PRACTISE

Secure identities across clouds	01
Protect networks and data	02
Detect and respond to cloud threats	03
Automate cloud security controls	04

✦ WHO IT'S FOR

Built for people ready to grow.

01

Beginners & non-tech roles

Cloud fundamentals, AWS CLF, AZ-900, GCP Digital Leader

02

Administrators & SysOps

AZ-104, SOA-C02, GCP ACE

03

Developers

AWS DVA-C02 and AZ-204

04

Architects

SAA, SAP, AZ-305, GCP PCA, multi-cloud

PREREQUISITES

Associate-level AWS or Azure experience	01
Solid security fundamentals: IAM, networking, encryption	02
Scripting experience in Python, Bash or PowerShell	03

ROLES YOU CAN TARGET

- Cloud Security Engineer ↗
- Cloud Security Architect ↗
- DevSecOps Engineer ↗
- Security Operations Engineer (Cloud) ↗
- Cloud Compliance Specialist ↗

✦ LEARNING OUTCOMES

What you'll be able to do.

01 Secure identities using least privilege across AWS IAM and Entra ID

02 Design secure cloud networks with segmentation and private access

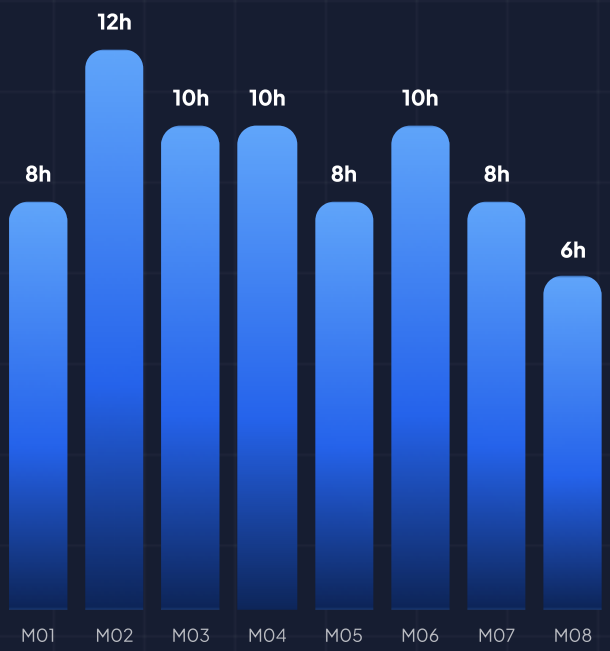
03 Protect data using encryption, key management and data classification

04 Detect threats with GuardDuty, Defender for Cloud and Sentinel

05 Respond to and investigate cloud security incidents effectively

06 Automate security controls with policy as code and IaC scanning

HOURS PER MODULE



✦ PROGRAM RUNWAY

Your journey, module by module.

8
MODULES · 72 HRS

01	**Cloud Security Foundations** Shared responsibility across AWS and Azure, Cloud threat landscape and attack paths, MITRE ATT&CK for Cloud	8 hrs
02	**Identity and Access Security** AWS IAM policies and permission boundaries, AWS IAM Identity Center and SCPs, Microsoft Entra ID and Conditional Access	12 hrs
03	**Network Security** VPC and VNet segmentation, Security groups, NACLs and NSGs, AWS Network Firewall and Azure Firewall	10 hrs
04	**Data Protection** Encryption at rest and in transit, AWS KMS and Azure Key Vault, Customer-managed keys and rotation	10 hrs
05	**Posture Management and Compliance** AWS Security Hub and Config, Microsoft Defender for Cloud secure score, CSPM and CNAPP concepts	8 hrs
06	**Threat Detection and Monitoring** CloudTrail and Azure Activity Logs, Amazon GuardDuty, Microsoft Sentinel and KQL	10 hrs
07	**Incident Response and Forensics** Cloud incident response lifecycle, Containment of compromised identities and instances, Evidence collection and snapshots	8 hrs
08	**Security Automation and DevSecOps** Policy as code: Azure Policy, SCPs, IaC scanning with Checkov, Open Policy Agent basics	6 hrs
★	**Capstone · Secure Multi-Cloud Environment Defence** Assessment, capstone review and certification	

✦ DETAILED CURRICULUM

The syllabus.

Modules 01–03

MODULE 01

Cloud Security Foundations

8 hours

Hands-on lab
Map common cloud attack paths to MITRE ATT&CK techniques.

TOPICS COVERED

- Shared responsibility across AWS and Azure
- Cloud threat landscape and attack paths
- MITRE ATT&CK for Cloud
- CIS Benchmarks and NIST CSF 2.0
- Secure landing zone principles

aws AWS

MODULE 02

Identity and Access Security

12 hours

Hands-on lab
Identify and remediate over-privileged identities using IAM Access Analyzer and Entra tools.

TOPICS COVERED

- AWS IAM policies and permission boundaries
- AWS IAM Identity Center and SCPs
- Microsoft Entra ID and Conditional Access
- Privileged Identity Management
- Workload identities and federation
- Detecting excessive permissions

aws AWS

MODULE 03

Network Security

10 hours

Hands-on lab
Build segmented networks with firewalls and private endpoints in both clouds.

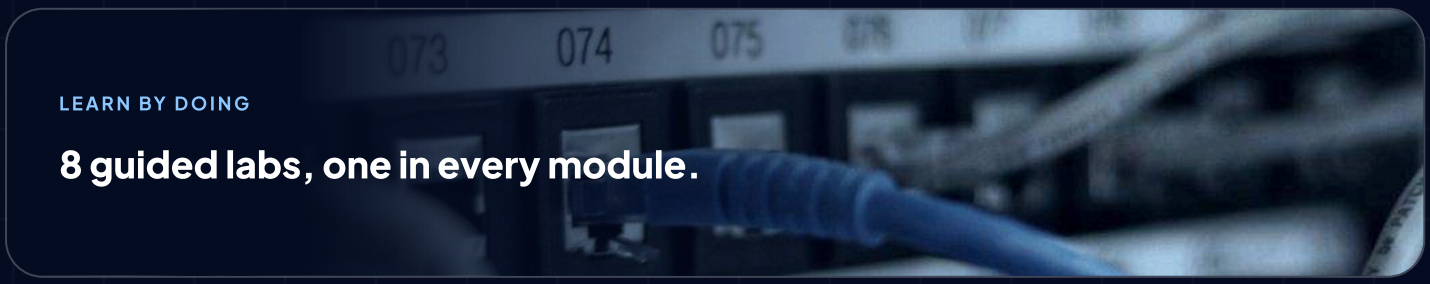
TOPICS COVERED

- VPC and VNet segmentation
- Security groups, NACLs and NSGs
- AWS Network Firewall and Azure Firewall
- Private endpoints and PrivateLink
- WAF and DDoS protection
- Zero Trust network access

aws AWS

LEARN BY DOING

8 guided labs, one in every module.



✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 04–06

MODULE 04

Data Protection

10 hours

Hands-on lab
Implement customer-managed keys and detect sensitive data with Macie.

TOPICS COVERED

- Encryption at rest and in transit
- AWS KMS and Azure Key Vault
- Customer-managed keys and rotation
- Secrets management
- Data classification with Macie and Purview
- Backup immutability and ransomware defence

aws AWS

MODULE 05

Posture Management and Compliance

8 hours

Hands-on lab
Assess both environments against CIS Benchmarks and remediate findings.

TOPICS COVERED

- AWS Security Hub and Config
- Microsoft Defender for Cloud secure score
- CSPM and CNAPP concepts
- Compliance frameworks and audits
- Workload and container security

aws AWS

MODULE 06

Threat Detection and Monitoring

10 hours

Hands-on lab
Build Sentinel analytics rules and investigate GuardDuty findings.

TOPICS COVERED

- CloudTrail and Azure Activity Logs
- Amazon GuardDuty
- Microsoft Sentinel and KQL
- Detection engineering basics
- Centralised logging architecture

LEARN BY DOING

8 guided labs, one in every module.



✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 07–08

MODULE 07

Incident Response and Forensics

8 hours

Hands-on lab
Respond to a simulated credential compromise and contain affected resources.

TOPICS COVERED

- Cloud incident response lifecycle
- Containment of compromised identities and instances
- Evidence collection and snapshots
- Automated response playbooks
- Post-incident reviews

MODULE 08

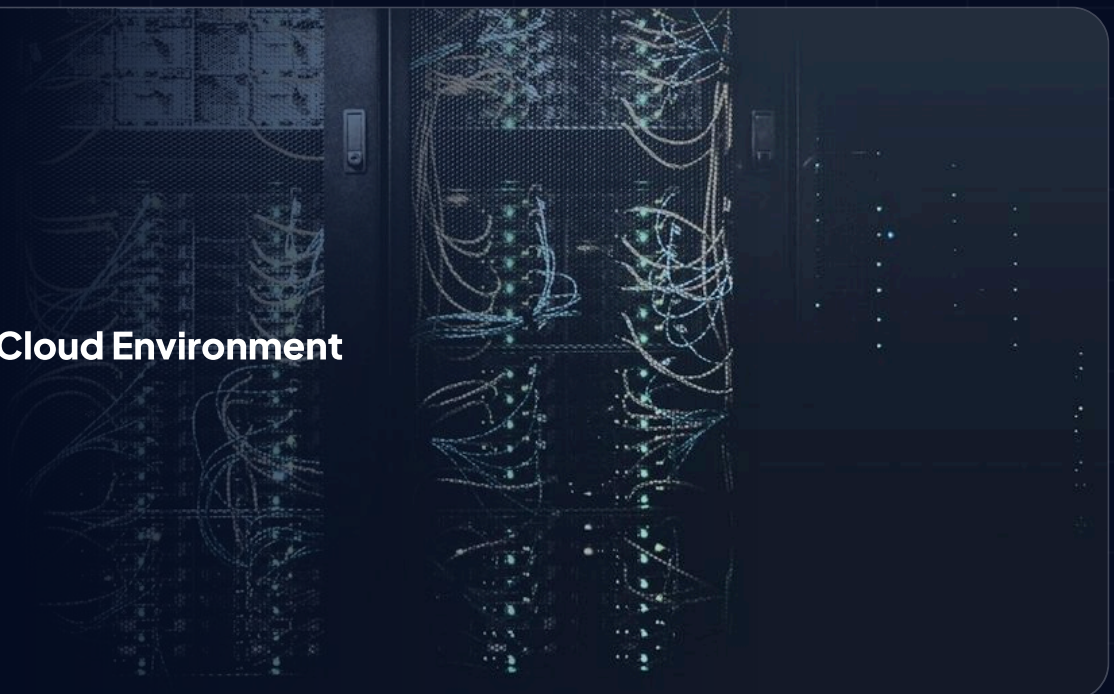
Security Automation and DevSecOps

6 hours

Hands-on lab
Add Checkov IaC scanning and auto-remediation to a deployment pipeline.

TOPICS COVERED

- Policy as code: Azure Policy, SCPs
- IaC scanning with Checkov
- Open Policy Agent basics
- Pipeline security controls
- Auto-remediation with Lambda and Logic Apps



CAPSTONE

Secure Multi-Cloud Environment Defence

✦ YOUR STACK

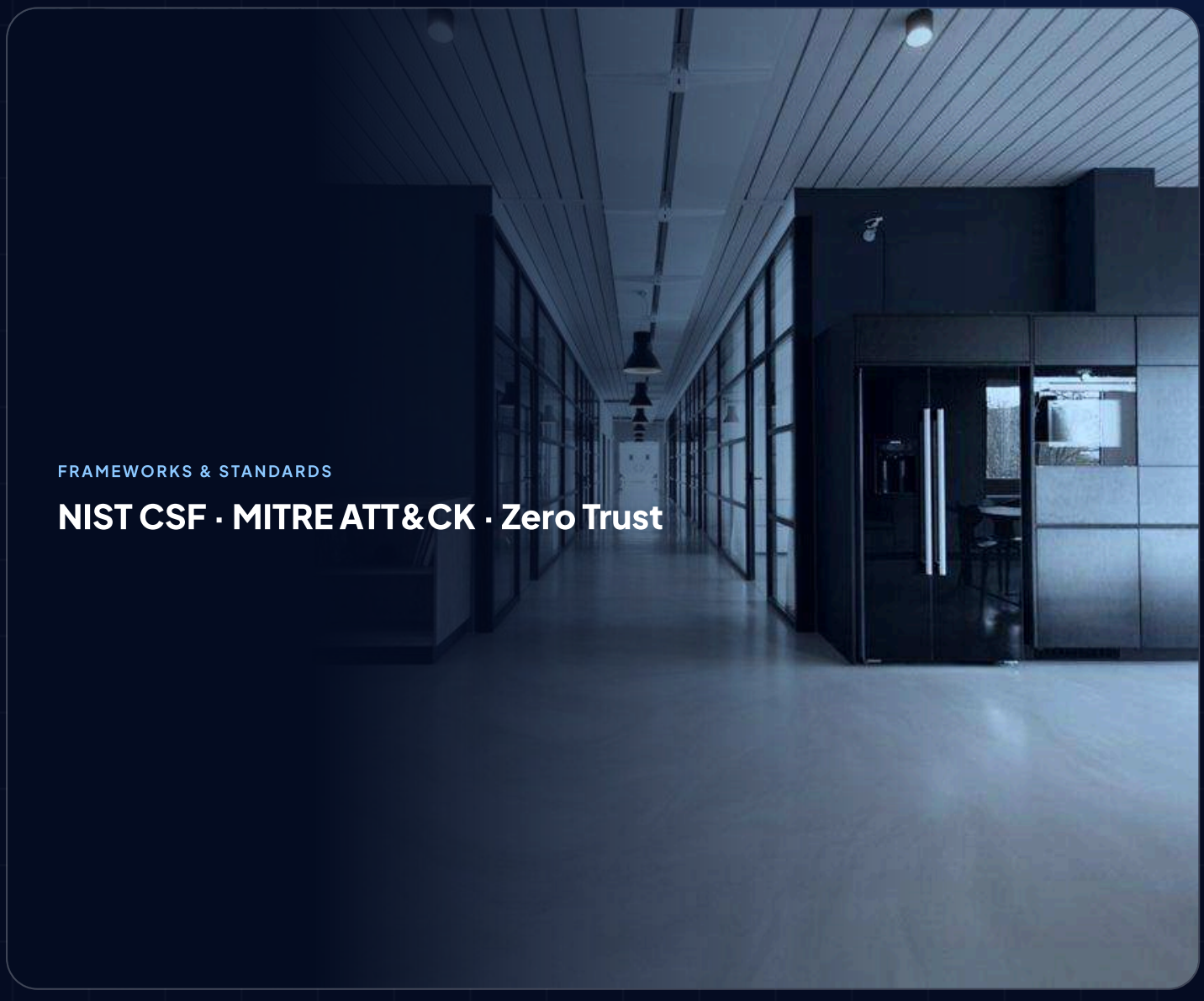
Tools you'll build with.

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

AWS
Cloud platform

Microsoft Azure
Cloud platform

Terraform
Infrastructure as code



FRAMEWORKS & STANDARDS

NIST CSF · MITRE ATT&CK · Zero Trust

✦ HANDS-ON WORK

Projects that prove you can do it.

01

Multi-Cloud Identity Hardening

Audit and harden identities across AWS and Azure, applying least privilege, MFA, Conditional Access and permission boundaries.

02

Threat Detection Lab

Configure GuardDuty, Defender for Cloud and Sentinel, simulate attacks and build detection and alerting rules.

03

Security-as-Code Pipeline

Integrate IaC scanning, policy as code and automated remediation into a CI/CD pipeline for both clouds.

CAPSTONE PROJECT

Secure Multi-Cloud Environment Defence

Design and harden an AWS and Azure environment covering identity, network, data and posture controls, then detect and respond to simulated attacks, automate remediation and deliver a security architecture and incident report.

Real-world scenario | Mentor review | Portfolio ready



CERTIFICATION

SAM-CLDSEC

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 · CLOUD COMPUTING

Where this program fits.

Beginner	Intermediate	Advanced	Expert
4 programs	6 programs	4 programs	You are here

BEFORE THIS

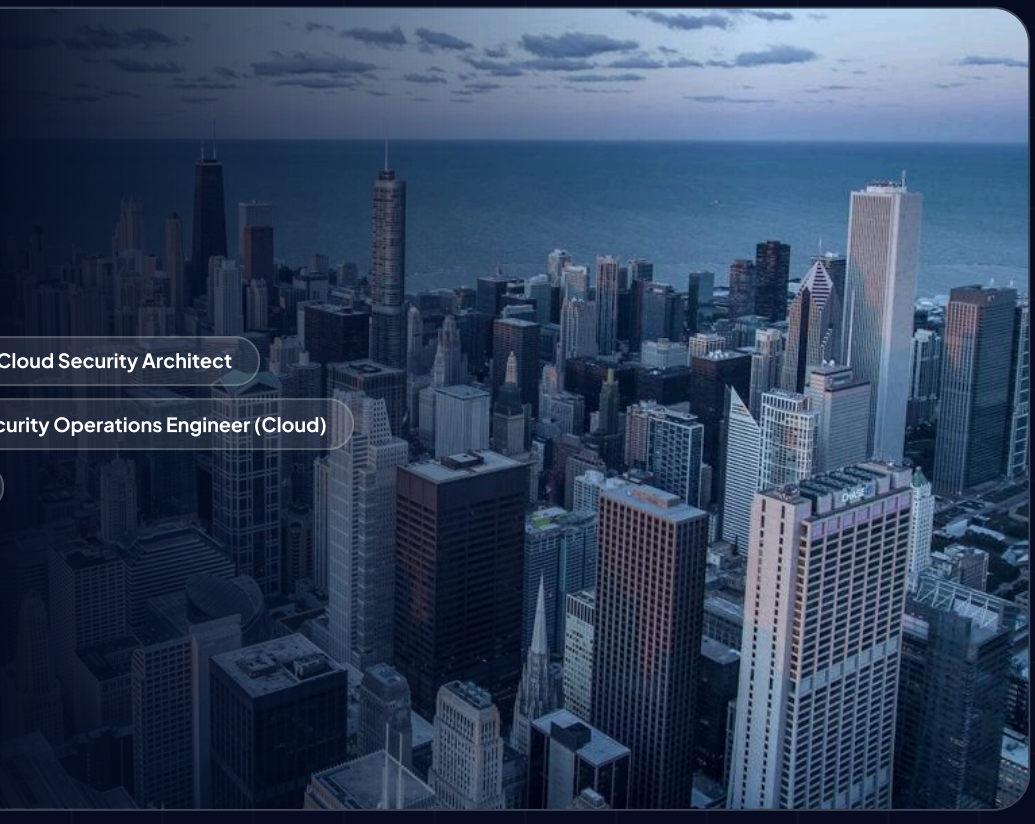
AWS Solutions Architect Professional (SAP-C02)	96 Hours
AWS DevOps Engineer Professional	96 Hours
Azure Solutions Architect (AZ-305)	96 Hours
GCP Professional Cloud Architect	96 Hours

UP NEXT

The top of this pathway — explore related tracks.

CAREER ROLES

- Cloud Security Engineer
- Cloud Security Architect
- DevSecOps Engineer
- Security Operations Engineer (Cloud)
- Cloud Compliance Specialist



✦ FAQS

Questions, answered.

Q01

Do I need prior experience?

Yes. This expert program requires associate-level experience with AWS or Azure and solid security fundamentals in identity, networking and encryption. Scripting skills are needed for automation labs. Foundational cloud programs are recommended otherwise.

Q02

How are classes scheduled and delivered?

Sessions are instructor-led and run as live virtual or blended batches, with weekday and weekend options where available. Concept sessions are followed by attack-and-defend labs, with notes and lab guides for revision.

Q03

Will I receive a certificate?

Yes. Learners who complete the required labs, projects and final assessment receive the Samcommunity Academy SAM-CLDSEC certificate. It recognises the practical skills you demonstrated during the program rather than attendance alone.

Q04

How do I access labs and tools?

Labs use AWS and Azure free-tier or sandbox accounts with isolated security lab environments. Instructors show how to set budgets and clean up resources to avoid unexpected charges, and step-by-step lab guides are shared for every module.

Q05

Is career support included?

You get guidance on portfolio projects, resume positioning and interview preparation for relevant roles. Security labs and reports can be documented as portfolio evidence. We do not guarantee jobs, placements or salaries.



✦ LET'S TALK

Start Cloud Security 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