Cloud & Application Security

Program Brochure · 2026

KUBERNETES SECURITY

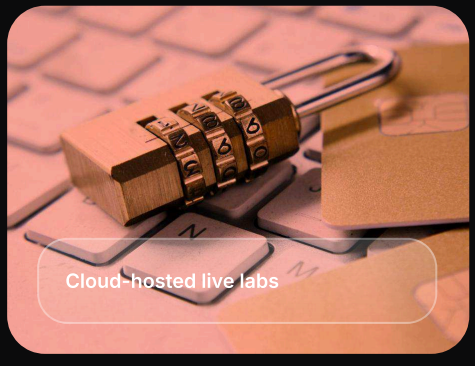
Lock down your clusters.

Advanced ↗ 40 Hours ↗ SAM-K8SSEC ↗

Cybersecurity

Cloud & Application Security

8 programs in this track



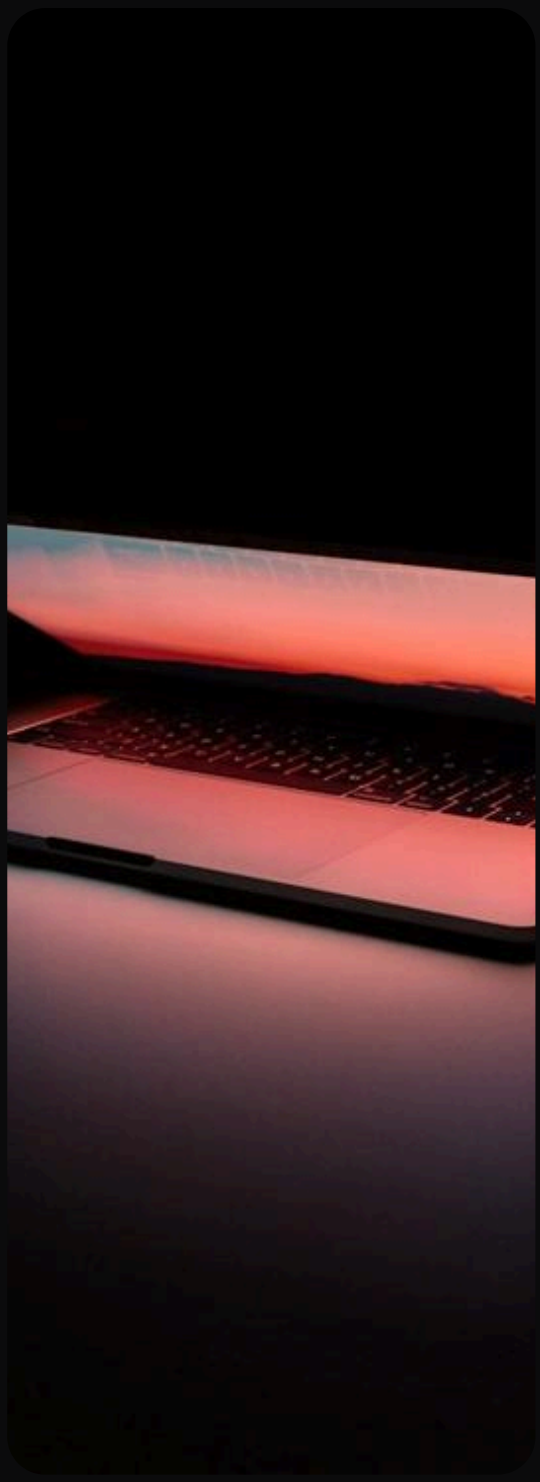
6

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	**40 Hours**
Modules	**6**
Certificate	**SAM-K8SSEC**

Program overview

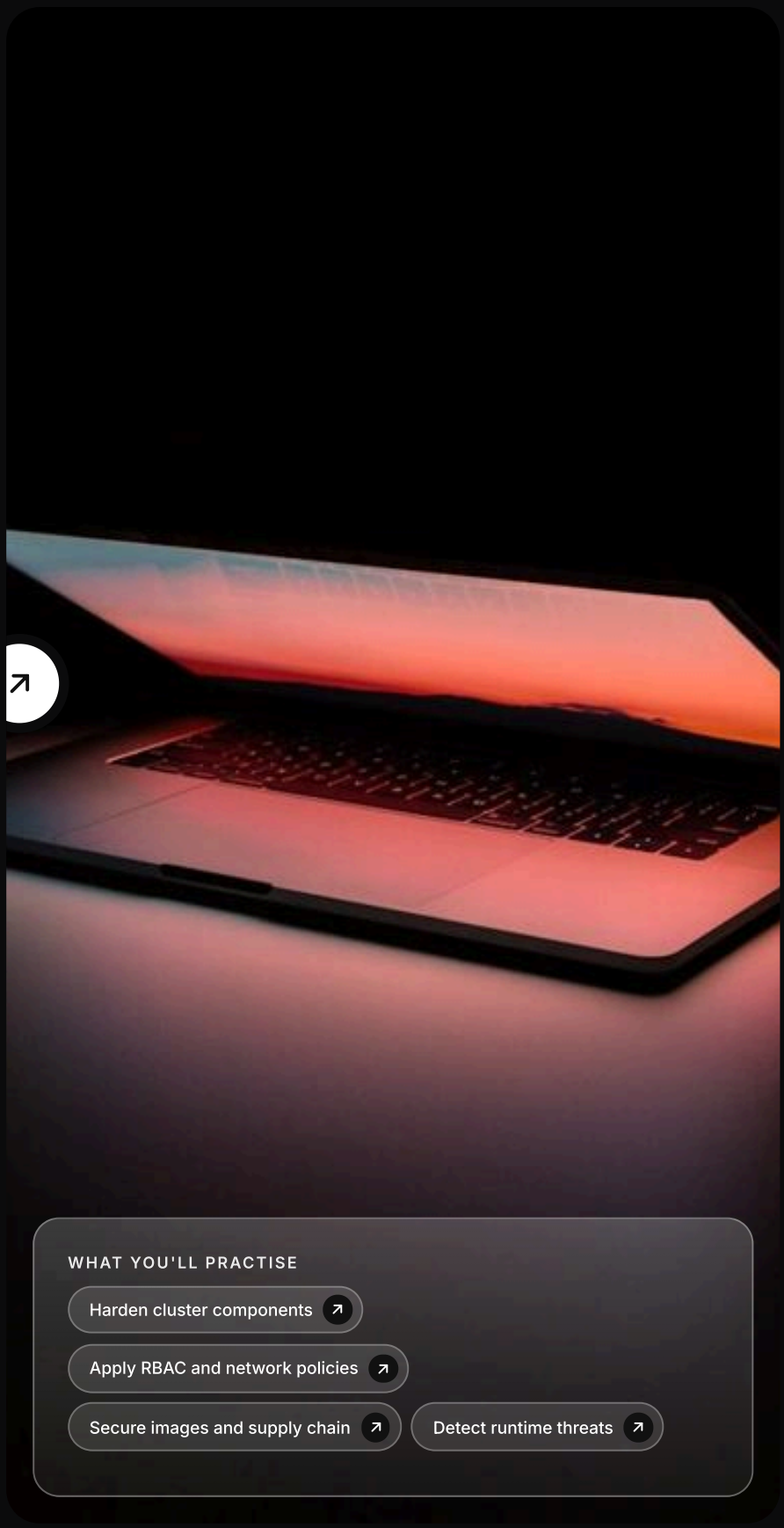
Lock down your clusters.

Secure Kubernetes clusters, workloads and supply chains — RBAC, network policies, admission control and runtime security.

Kubernetes runs modern production workloads, and its flexibility creates a wide attack surface if misconfigured. This advanced program teaches you to secure clusters, workloads and supply chains, covering RBAC, network policies, admission control and runtime security. You finish able to harden cluster components, enforce least privilege and detect threats in running workloads with confidence.

DELIVERY

Instructor-led · Live virtual · Blended



WHAT YOU'LL PRACTISE

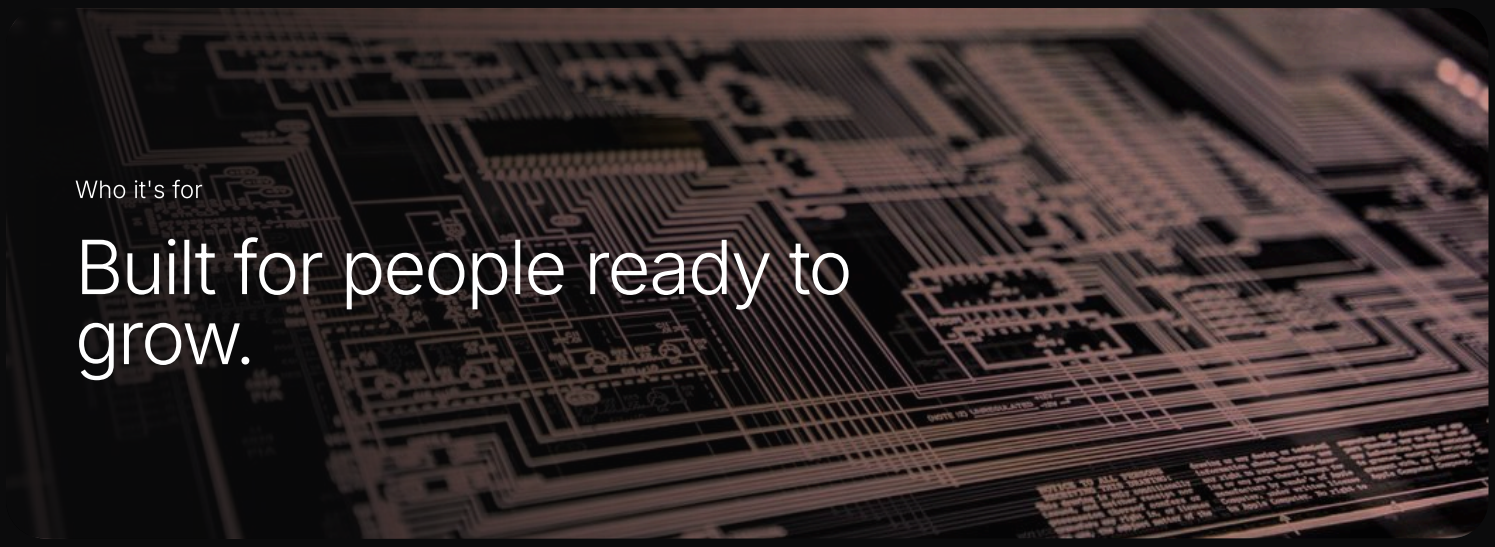
- Harden cluster components
- Apply RBAC and network policies
- Secure images and supply chain
- Detect runtime threats

LEVEL
Advanced

DURATION
40 Hours

CERTIFICATION
SAM-K8SSEC

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

Working knowledge of Kubernetes basics	01
Familiarity with containers and Docker	02
Comfort with the Linux command line	03

ROLES THIS PREPARES YOU FOR

- Kubernetes Security Engineer ↗
- Platform Engineer ↗
- Cloud Security Engineer ↗
- DevSecOps Engineer ↗
- Site Reliability Engineer ↗
- Container Security Specialist ↗

Learning outcomes

What you'll be able to do.



01	Harden Kubernetes cluster components against common threats
02	Design role-based access control with least privilege
03	Enforce network policies to isolate cluster workloads
04	Apply admission control and policy engines effectively
05	Secure container images and the software supply chain
06	Detect and respond to runtime threats in clusters

Program runway

Module by module.

6
modules · 40 hours

01	**Kubernetes Security Foundations** Cluster architecture, Attack surface overview, Threat model	6 hrs
02	**RBAC and Access Control** RBAC design, Service accounts, Least privilege roles	8 hrs
03	**Network and Workload Security** Network policies, Pod security standards, Secrets management	8 hrs
04	**Admission Control and Policy** Admission controllers, Policy engines, Validating policies	6 hrs
05	**Image and Supply Chain Security** Image scanning, Image signing, Registry security	6 hrs
06	**Runtime Security and Response** Runtime threat detection, Behavioural monitoring, Audit logging	6 hrs
★	**Capstone · Secure Kubernetes Platform** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Kubernetes Security Foundations

6 hours

Hands-on lab
Run a CIS benchmark review against a sample cluster configuration

TOPICS COVERED

- Cluster architecture
- Attack surface overview
- Threat model
- Security benchmarks
- 4C security model
- Tooling landscape

Kubernetes

Module 02

RBAC and Access Control

8 hours

Hands-on lab
Design and test least-privilege RBAC roles for a sample namespace

TOPICS COVERED

- RBAC design
- Service accounts
- Least privilege roles
- API server security
- Authentication methods
- Access auditing

Module 03

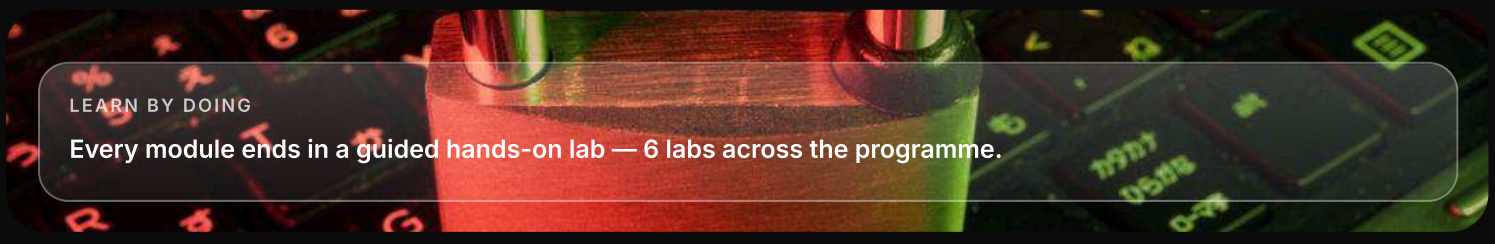
Network and Workload Security

8 hours

Hands-on lab
Apply network policies and pod security standards to isolate workloads

TOPICS COVERED

- Network policies
- Pod security standards
- Secrets management
- Workload isolation
- Security contexts
- Namespace strategy



LEARN BY DOING

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

Syllabus, continued.

Modules 04–06

Module 04

Admission Control and Policy

6 hours

Hands-on lab
Enforce an admission policy that blocks risky workload configurations

TOPICS COVERED

- Admission controllers
- Policy engines
- Validating policies
- Guardrail design
- Deployment gating
- Exceptions management

Module 05

Image and Supply Chain Security

6 hours

Hands-on lab
Enforce a policy that blocks unsigned or vulnerable container images

TOPICS COVERED

- Image scanning
- Image signing
- Registry security
- Supply chain integrity
- Provenance checks
- Trusted sources

Module 06

Runtime Security and Response

6 hours

Hands-on lab
Detect and investigate a simulated runtime threat in a lab cluster

TOPICS COVERED

- Runtime threat detection
- Behavioural monitoring
- Audit logging
- Incident response
- Forensics basics
- Continuous hardening



CAPSTONE

Secure Kubernetes Platform



Kubernetes
Container orchestration

Docker
Containers & images

Helm
Kubernetes packaging

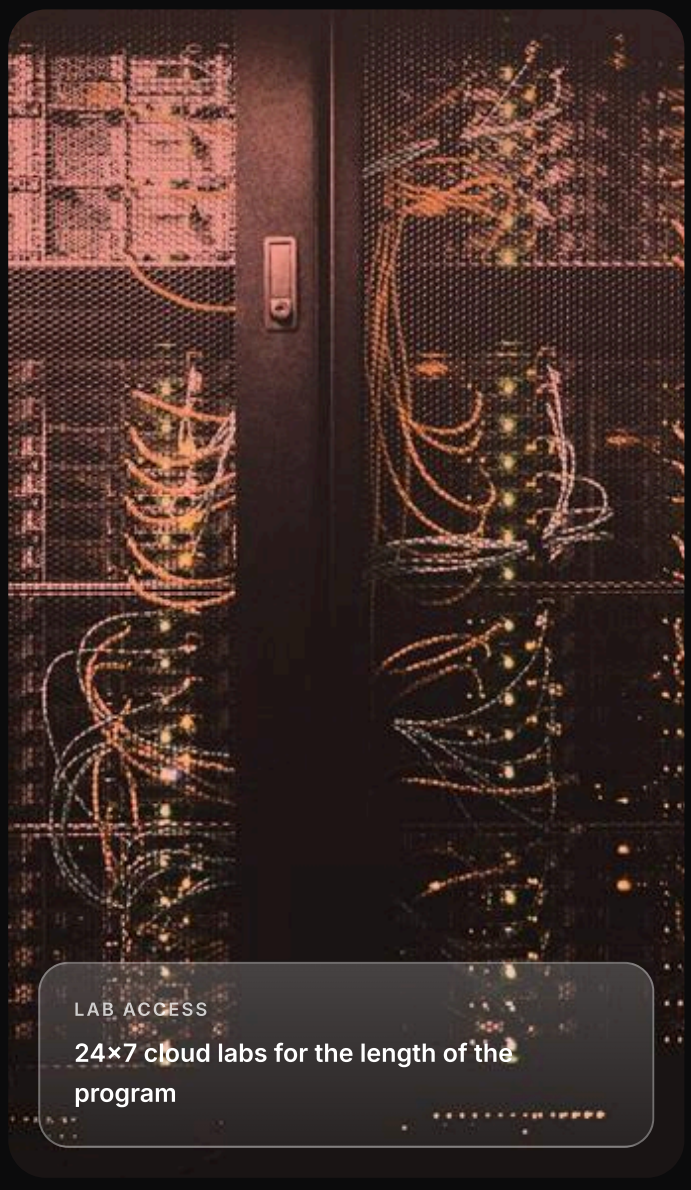
Linux
Server & CLI fundamentals

Frameworks & standards

- MITRE ATT&CK
- NIST CSF
- ISO 27001

FOCUS AREAS

Harden cluster components	01
Apply RBAC and network policies	02
Secure images and supply chain	03
Detect runtime threats	04



01

Cluster Hardening

Harden a sample Kubernetes cluster against a security benchmark, documenting the configuration changes and the risks each one addresses.

02

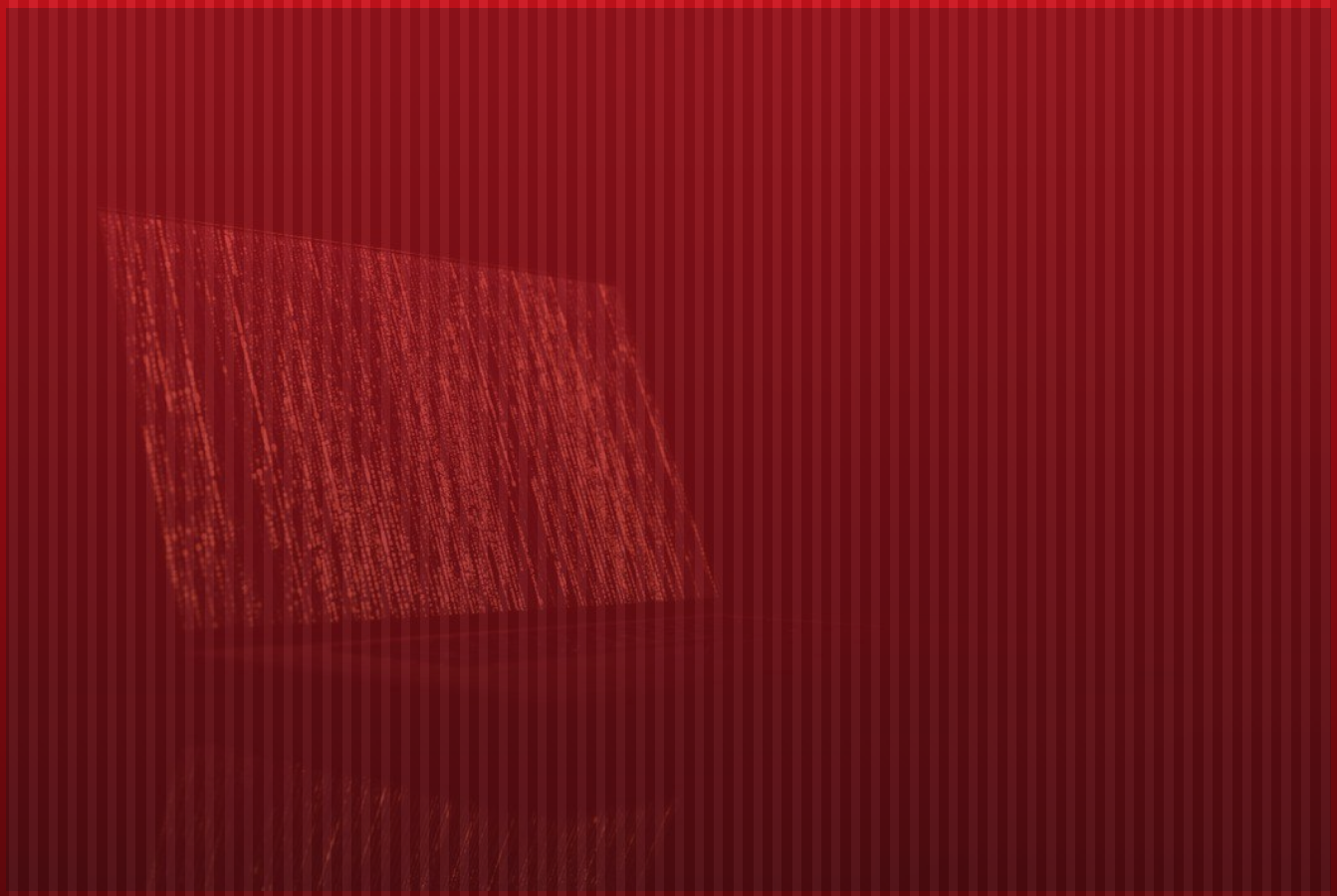
RBAC and Network Policy Design

Design least-privilege RBAC and network policies for a multi-team cluster, then test that workloads are correctly isolated.

03

Supply Chain Guardrails

Implement admission control and image policies that block unsigned or vulnerable images from being deployed to a sample cluster.



Capstone project

Secure Kubernetes Platform

Secure a complete sample Kubernetes platform end to end, applying cluster hardening, least-privilege RBAC, network policies, admission control and runtime detection, then document the design and demonstrate detection of a simulated attack.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-K8SSEC

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

- Kubernetes Security Engineer
- Platform Engineer
- Cloud Security Engineer
- DevSecOps Engineer
- Site Reliability Engineer

Questions, answered.

Q01

Do I need prior experience to join?

Yes. You should already know Kubernetes basics and be comfortable with containers, Docker and the Linux command line before joining, as this advanced course focuses on hardening, access control and runtime defence rather than teaching core Kubernetes concepts from scratch.

Q02

How is the program delivered and scheduled?

The 40-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-K8SSEC 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 KUBERNETES 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