

Module 5: Specialisation & Cloud Security

80 hrs · R10,500 · 4 weeks

The cloud is where the next generation of threats lives. This cloud security course teaches you to secure AWS and Azure environments in South Africa, apply DevSecOps principles, harden Docker containers and CI/CD pipe...

80 hrs

Training Hours

R10,500

Module Fee

4 weeks

Full-Time

8 weeks

Part-Time

JHB · Online

Delivery

WEEKLY CURRICULUM

What You'll Learn

AWS & Azure Security Fundamentals

Cloud architecture review (IAM, VPC/VNet, storage, compute). AWS security services: GuardDuty, Security Hub, CloudTra...

Cloud Attacks & Defences

Common cloud misconfigurations: public S3 buckets, over-permissive IAM roles, IMDSv1 SSRF. Server-side request forger...

DevSecOps & Secrets Management

Security in CI/CD: SAST (Semgrep), DAST (OWASP ZAP), Software Composition Analysis (SCA). Secrets management with Has...

Elective Specialisation & Exam Prep

Students choose: PenTest+ (PT0-003) — advanced pen testing methodology, planning, scoping, legal, reporting; or Cloud...

LEARNING OUTCOMES

After This Module You Will Be Able To

- ✓ Audit and harden AWS and Azure environments using native security services (GuardDuty, Sentinel, CloudTrail)
- ✓ Identify and exploit common cloud misconfigurations (SSRF, IMDSv1, public S3) in a controlled lab
- ✓ Apply DevSecOps practices: integrate security into CI/CD pipelines, scan container images and IaC templates
- ✓ Implement secrets management with HashiCorp Vault — eliminating hard-coded credentials
- ✓ Choose and demonstrate readiness for CompTIA PenTest+ (offensive) or Cloud+ (defensive) certification
- ✓ Apply POPIA (SA) and GDPR data protection requirements to cloud-hosted workloads

TOOLS & PLATFORMS

AWS Free Tier

Azure Free Account

Prowler (cloud security scanner)

CloudGoat (AWS attack lab)

Docker + Falco

HashiCorp Vault

Semgrep / OWASP ZAP

Checkov (IaC scanning)

TryHackMe (Cloud path)

Certification Alignment

This module prepares you for the following internationally recognised exams. Exam fees are separate.

CompTIA PenTest+ / Cloud+

AWS & Azure Security

WHAT TO EXPECT

Your Learning Experience



Expert-Led Live Training

Live sessions, not recordings. Taught by industry practitioners with 20+ years of training experience.



Hands-On VM Labs

Every topic has a lab exercise. You build, break and defend real systems in your own VM environment.



Johannesburg & Online

In-person at Code College Woodmead or 100% live online from anywhere in South Africa.



Digital Badge on Completion

Earn a Code College Digital Badge — shareable to LinkedIn. Stack badges toward the full bootcamp certificate.

2026 PRICING

Investment

MODULE FEE

R10,500

One flat price — no hidden fees

TRACK BUNDLE (3 MODULES)

From R26,500

Save up to R4,500 vs individual prices

Get in Touch

 info@codecollege.co.za

 +27 (0)10 970 7777

 WhatsApp: +27 83 600 2765

 codecollege.co.za/short-cybersecurity-courses/module-5-cloud-security/

Payment plans available · Group rates on request · EFT & card accepted · B-BBEE Level 4

FAQS

Frequently Asked Questions

Q Do I need an AWS or Azure account?

Yes. Both platforms offer free tier accounts — AWS Free Tier and Azure Free Account — which are sufficient for all lab exercises in this module. We guide you through account setup on day one. Total cloud spend during the module is typically under R50 if you follow the lab guides and terminate resources after each session.

Q How do I choose between PenTest+ and Cloud+ as my elective?

If your goal is an offensive/red team role (pen tester, red team analyst, bug bounty hunter), choose PenTest+. If you are aiming for a cloud security, GRC, DevSecOps or compliance role, choose Cloud+. Both are valid pathways and the first three weeks of this module are identical regardless of which elective you pick. Your instructor can help you decide during Week 2.

Q Is this module useful even if I don't plan to work in cloud security?

Yes. Almost every SA employer now runs at least some workloads in the cloud. Understanding cloud security architecture, IAM policies and DevSecOps practices has become a baseline expectation even for on-premise security roles. This module closes the cloud knowledge gap that many Security+ holders have.

Q Can I take Module 5 before Module 3 or 4?

No — Module 5 requires either Module 3 or Module 4 as a prerequisite. The cloud attack labs in Week 2 build on exploitation techniques from Module 3, and the Azure Sentinel and monitoring work extends the SIEM skills from Module 4. Taking Module 5 without this foundation would significantly reduce the value of the practical labs.

Q What is the difference between CompTIA PenTest+ and CEH?

CEH (Module 3) emphasises attack methodology and hacker mindset — it is widely recognised by financial services employers globally and in South Africa. CompTIA PenTest+ emphasises planning, scoping, legal constraints and formal pen test reporting — it is DoD-approved and required for US government-adjacent contracts. PenTest+ is also cheaper to sit. Many students pursue both: CEH for market recognition, PenTest+ for compliance coverage in regulated environments.

Next Step in Your Cybersecurity Journey

Next step: Module 6 — Portfolio & Job Readiness →