

Module 4: Blue Team & SOC Operations

100 hrs · R12,000 · 5 weeks

The defender's discipline. This SOC analyst training course teaches you to monitor, detect, investigate and respond to real-world cyber threats — using the same tools as professional security operations centres....

100 hrs

Training Hours

R12,000

Module Fee

5 weeks

Full-Time

10 weeks

Part-Time

JHB · Online

Delivery

WEEKLY CURRICULUM

What You'll Learn

Security Monitoring & SIEM Deployment

SIEM architecture and log management fundamentals. Deploy Security Onion in your VM lab. Configure log sources: Zeek ...

Threat Intelligence & Threat Hunting

MITRE ATT&CK framework: tactics, techniques and procedures (TTPs). Sigma rules for detection engineering. Threat ...

Incident Response & Digital Forensics

The IR lifecycle: Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned. Memory forensics ...

Vulnerability Management

Nessus credentialed and uncredentialed scanning. CVSS v3.1 scoring and risk prioritisation. Patch management workflow...

Splunk SIEM & CySA+ Exam Prep

Splunk architecture, log ingestion via forwarders, SPL (Search Processing Language) fundamentals, correlation rules, ...

LEARNING OUTCOMES

After This Module You Will Be Able To

- ✓ Deploy and operate Security Onion as a full network security monitoring platform in a VM lab
- ✓ Analyse Zeek logs and Suricata alerts to identify active intrusions and suspicious network behaviour
- ✓ Perform a structured incident response including memory forensics with Volatility
- ✓ Build Splunk dashboards with SPL queries for real-time threat detection
- ✓ Conduct vulnerability management using Nessus, CVSS scoring and CIS Benchmark compliance checks
- ✓ Demonstrate CompTIA CySA+ (CS0-003) exam readiness across all four exam domains

TOOLS & PLATFORMS

Security Onion

Zeek (Bro)

Suricata

Splunk SIEM

Volatility (memory forensics)

FTK Imager

Nessus

Wireshark

MITRE ATT&CK Navigator

TryHackMe (SOC Level 1 path)

Certification Alignment

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

CompTIA CySA+ (CS0-004)

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

R12,000

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-4-blue-team-soc/

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

FAQS

Frequently Asked Questions

Q What hardware do I need for Module 4?

No specific hardware required. Module 4 runs entirely in your browser: Security Onion, Splunk, Elastic SIEM, and live threat simulation labs all run on Code College's Docker infrastructure. Minimum: any laptop with 4 GB RAM, a web browser, and stable internet (10+ Mbps). That's it. No local VMs, no resource constraints, no setup needed.

Q What is the difference between CySA+ and Security+?

Security+ (Module 2) is a broad baseline covering policy, compliance and general threat awareness. CySA+ (CS0-003) is the next step — it focuses specifically on applying behavioural analytics, threat intelligence and incident response at the analyst level. CySA+ assumes you already hold Security+ or equivalent knowledge, which is why Module 2 is the prerequisite.

Q What salary can a CySA+ holder earn in South Africa?

A certified SOC Analyst (L1/L2) with CySA+ can expect R300,000–R700,000 p.a. in South Africa as of 2026. L2 incident responders with 1–2 years' experience typically earn R700,000–R800,000 p.a. Financial sector employers (banks, insurers) tend to pay at the higher end. Remote roles for UK/EU employers are increasingly available at £35,000–£50,000 p.a.

Q Does this module use real-world attack simulations?

Yes. Week 2 (Threat Hunting) and Week 5 (Splunk) use pre-recorded attack scenarios — PCAP captures and log datasets from real incidents — that you analyse as if responding live. Week 4 includes a simulated incident response scenario where you receive an alert, investigate with Volatility and Zeek, and produce a formal IR report.

Q Can I use SDL funding for CompTIA CySA+ training?

CySA+ training aligns to an internationally recognised CompTIA certification and can be included as a planned skills development expense in your company's Workplace Skills Plan. Contact us for a formal quotation suitable for WSP submission.

Next Step in Your Cybersecurity Journey

Next step: Module 5 (Cloud Security) or Module 6 (Portfolio & Career) →