🔒 Cybersecurity Bootcamp · Specialist Track

CODE COLLEGE

SOC Analyst Track

ISC² CC · CompTIA Network+ · CompTIA Security+ (SY0-701) · CompTIA CySA+ (CS0-003)

South Africa's most in-demand cybersecurity role. The SOC Analyst Track trains you to monitor, detect, investigate and respond to real-world cyber threats — using the same tools and workflows as professional security operations centres. Graduate with CySA+ exam rea...

Splunk · Microsoft Sentinel · Security Onion · Zeek · Suricata · Volatility · FTK Imager · Wireshark · SOAR

260 hrs	3	4	~3 Months	R28,000
Training	Modules	Certs Aligned	Full-Time	Track Fee

WHAT'S IN THIS TRACK

Three Modules. One Career Path.

M1

IT & Networking Foundations

ISC² CC · CompTIA Network+

Build a rock-solid networking foundation. OSI & TCP/IP models, subnetting, DNS, DHCP, Wireshark packet analysis and your first Kali Linux lab setup. No prior experience required.

R9,500 80 hours

M2

Core Security Fundamentals

CompTIA Security+ SY0-701

Master the security essentials. Threats and vulnerabilities, cryptography, PKI, firewalls, IDS/IPS, vulnerability scanning, identity management, and compliance frameworks including POPIA and NIST.

R10,500 80 hours

M4

Blue Team & SOC Operations

CompTIA CySA+ CS0-003

Deploy and operate a full SIEM stack. Threat hunting, detection engineering, incident response, digital forensics, Splunk dashboards, Microsoft Sentinel and SOAR automation playbooks.

R12,000 100 hours

info@codecollege.co.za · +27 (0)10 970 7777 · WhatsApp: +27 83 600 2765

CURRICULUM HIGHLIGHTS

Week-by-Week Training

WEEKS 1–2
Networking Foundations
OSI model, TCP/IP stack, DNS, DHCP, routing and switching fundamentals. Build the networking knowledge every SOC analyst depends on.

WEEKS 3–4
Network Tools & Lab Setup
Wireshark packet captures, Kali Linux installation, virtual machine configuration. Set up your personal security lab environment.

WEEKS 5–6
Security Concepts & Threat Landscape
Threat actors, attack vectors, malware types, social engineering and the cyber kill chain. Understand what you will be defending against.

WEEKS 7–8
Cryptography, PKI & Access Control
Symmetric and asymmetric encryption, hashing, digital certificates, PKI infrastructure and identity access management.

WEEKS 9–10
Firewalls, IDS/IPS & Vulnerability Scanning
Configure firewalls, deploy intrusion detection and prevention systems, run vulnerability scans with Nessus and OpenVAS.

WEEKS 11–13
SIEM Deployment & Log Analysis
Deploy Splunk and Microsoft Sentinel. Ingest and normalise logs, create dashboards, write detection rules and build correlation searches.

WEEKS 14–15
Threat Hunting & Detection Engineering
Proactive threat hunting with Zeek, Suricata and Security Onion. Write custom detection rules, analyse network traffic patterns and identify indicators of compromise.

WEEKS 16–17
Incident Response & Digital Forensics
IR playbooks, evidence acquisition, memory analysis with Volatility, disk imaging with FTK Imager, chain of custody and forensic reporting.

WEEK 18
SOC Reporting, Playbooks & SOAR Automation
Build SOC runbooks and standard operating procedures. Configure SOAR automation workflows. Capstone: end-to-end incident response exercise with full reporting.

CERTIFICATIONS ALIGNED

Industry Certifications

ISC² CC
Entry-level security certification from ISC². Validates foundational cybersecurity knowledge and opens the door to the ISC² professional pathway.

CompTIA Network+
Networking skills foundation for security professionals. Covers infrastructure, troubleshooting and the network knowledge every SOC analyst needs.

CompTIA Security+SY0-701
The gold standard entry-level security certification. Recognised worldwide by employers, government agencies and defence contractors.

CompTIA CySA+CS0-003
The defensive security certification purpose-built for SOC analysts. Validates threat detection, analysis, incident response and security monitoring skills.

WHO IS THIS FOR

Built for Your Career Path

Detail-Oriented Defenders

You're methodical, analytical and enjoy investigating problems. You want a cybersecurity career focused on defence, detection and response rather than offensive hacking.

- ✓No prior IT experience required — Module 1 starts from zero
- ✓Ideal for career changers drawn to security monitoring
- ✓Strong fit if you enjoy data analysis and pattern recognition
- ✓Build a portfolio of real incident response reports

IT Professionals Moving to Blue Team

You're already in IT — helpdesk, networking, system administration — and you want to pivot into security operations. This track formalises your knowledge and adds the SOC-specific skills employers require.

- ✓Skip Module 1 if you can pass the networking assessment
- ✓Security+ and CySA+ certify what you already know
- ✓Hands-on Splunk, Sentinel and SOAR lab experience
- ✓Part-time option — keep your current role while you upskill

CAREER OUTCOMES

Where This Track Takes You

SOC Analyst (Tier 1/2) | Threat Hunter | Incident Responder | Security Monitoring Analyst | SIEM Engineer | Digital Forensics Analyst

ENTRY-LEVEL	MID-LEVEL	SENIOR / LEAD
R400K – R700K	R800K – R1.2M	R1.2M – R2M+

PRICING

Track Pricing

Best Value

SOC Analyst Track (Bundle)

- ✓M1: IT & Networking Foundations (80 hours)
- ✓M2: Core Security Fundamentals (80 hours)
- ✓M4: Blue Team & SOC Operations (100 hours)

M1: IT & Networking Foundations	M2: Core Security Fundamentals	M4: Blue Team & SOC Operations
R9,500	R10,500	R12,000

FAQS

Frequently Asked Questions

Q Do I need IT experience to start the SOC Analyst Track?

No prior IT or cybersecurity experience is required. The SOC Analyst Track begins with Module 1 — IT & Networking Foundations — which starts from absolute zero. You will learn networking, Linux and set up your own home lab before progressing to security and SOC operations. If you already have an IT background, you may be able to skip Module 1 after a short assessment.

Q Which certifications does the SOC Analyst Track prepare me for?

The SOC Analyst Track prepares you for four internationally recognised certifications: ISC² Certified in Cybersecurity (CC), CompTIA Network+, CompTIA Security+ (SY0-701) and CompTIA CySA+ (CS0-003). Each module includes mock exams and exam-aligned content so you are fully prepared before sitting the official exam.

Q How long does the SOC Analyst Track take?

The SOC Analyst Track is 260 training hours across three modules. Full-time students typically complete the track in approximately 3 months. Part-time students can complete it in roughly 6 months. All sessions are recorded for catch-up, and you have a 24-month window to complete your modules.

Q Are certification exam fees included?

Exam fees are not included in the track fee. Your tuition covers all training materials, lab environments and mock exams to prepare you fully before you sit the official certification exam. Exam vouchers can be purchased at additional cost. The Professional and Elite bootcamp tiers include exam vouchers if you prefer a bundled option.

Q What tools will I learn in the SOC Analyst Track?

You will gain hands-on experience with the same tools used in professional security operations centres: Splunk and Microsoft Sentinel for SIEM, Security Onion for network security monitoring, Zeek and Suricata for network detection, Wireshark for packet analysis, Volatility and FTK Imager for digital forensics, and SOAR platforms for automated incident response.

Q What does a SOC analyst earn in South Africa?

Entry-level SOC analysts in South Africa earn between R400,000 and R700,000 per year. Mid-level analysts with CompTIA CySA+ or equivalent experience earn R800,000 to R1.2 million. Senior SOC analysts, threat hunters and incident response leads can earn R1.2 million to R2 million or more. Cybersecurity remains one of the highest-demand, highest-paying IT career paths in South Africa.

🏅 Want All Six Modules?

Complete all six modules across all three specialist tracks for the full Cybersecurity Bootcamp Certificate. Three tier options available.

STANDARD	PROFESSIONAL	ELITE
R49,500	R59,000	R79,000

Get in Touch

info@codecollege.co.za · +27 (0)10 970 7777 · WhatsApp: +27 83 600 2765

codecollege.co.za/cybersecurity-bootcamps/

Payment plans available · Group rates on request · EFT & card accepted · B-BBEE Level 4 · SDL eligible · Exam fees not included