Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

DEFENSE AND SECURITY

Certified SOC Analyst Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Certified SOC Analyst Training Course

Defense and Security • 5 Days Intensive • Accredited Certification

Course Overview

Certified SOC Analyst Training Course equips learners with the essential competencies required to operate effectively in a SOC environment, including threat monitoring, log analysis, event triage, SIEM operations, and incident response techniques.

Key Skills & Software Tools Covered

MS Word • Splunk • Wireshark • and AlienVault USM

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
29 Dec 2025 – 2 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
29 Dec 2025 – 2 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Accra	Classroom / 5d	**$4,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
5 Jan 2026 – 9 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Certified SOC Analyst Training Course

Introduction

Security Operations Centers (SOCs) play a critical role in safeguarding organizational systems, detecting cyber threats, and responding to security incidents in real time. As global cyber risks escalate and attackers deploy more advanced techniques, modern SOC analysts must possess strong analytical skills, deep technical knowledge, and the ability to interpret cybersecurity events with accuracy and speed. Certified SOC Analyst Training Course equips learners with the essential competencies required to operate effectively in a SOC environment, including threat monitoring, log analysis, event triage, SIEM operations, and incident response techniques. It integrates highly relevant cybersecurity keywords such as real-time threat detection, digital forensics, attack surface monitoring, and security automation.

This training offers an immersive learning experience that strengthens participants' ability to evaluate risks, understand attacker behavior, and coordinate effective incident escalation. Through practical exercises, hands-on investigation scenarios, and realistic case studies, participants gain the confidence to contribute directly to SOC operations. The course emphasizes actionable skills, including SIEM configuration, alert prioritization, security controls optimization, and continual improvement strategies that support organizational resilience. By the end, learners will be prepared to handle real-world cyber threats with professionalism and technical proficiency.

Course Objectives

- Understand foundational SOC concepts and modern cybersecurity threat landscapes.
- Analyze security events and logs using trending cybersecurity tools.
- Apply threat intelligence for proactive threat detection and early warning.
- Conduct effective event triage and prioritize high-risk alerts.
- Perform incident response tasks aligned with best practices and frameworks.
- Identify network-based threats using packet inspection and traffic analysis.
- Configure and optimize SIEM platforms for enhanced monitoring.
- Evaluate attacker tactics, techniques, and procedures using MITRE ATT&CK.
- Conduct root-cause investigations and prepare clear incident reports.
- Strengthen organizational cyber hygiene and endpoint security posture.
- Utilize automation and SOAR technologies for increased SOC efficiency.
- Detect anomalies through behavioral analytics and pattern recognition.
- Implement continuous improvement processes within SOC teams.

Organizational Benefits

- Strengthened cybersecurity monitoring capabilities
- Faster detection and response to cyber threats
- Reduced incident impact and operational disruption
- Improved cyber defense through skilled SOC personnel
- Enhanced use of SIEM and automated monitoring tools
- Lower organizational risk from advanced cyberattacks
- Increased operational resilience and data protection
- Better coordination during incident escalation
- Compliance with security standards and frameworks
- Stronger security culture across departments

Target Audiences

- SOC analysts and cybersecurity technicians
- IT security monitoring teams
- Cybersecurity operations staff
- Junior incident responders
- Security administrators and network analysts
- Digital forensics trainees
- Cybersecurity students preparing for SOC roles
- Professionals entering cyber defense fields

Course Duration: 5 days

Course Modules

Module 1: Introduction to SOC Operations

- Overview of SOC structures, functions, and components
- Roles and responsibilities of SOC teams
- SOC maturity models and operational workflows
- Overview of cyber threats affecting SOC environments
- Introduction to SOC technologies and monitoring tools
- Case Study: Building a SOC from the ground up

Module 2: SIEM Platforms & Log Management

- Understanding SIEM architecture and features
- Configuring log collection and event correlation rules
- Performing log analysis and alert investigations
- Customizing dashboards for effective monitoring
- Reducing false positives through filtering optimization
- Case Study: SIEM misconfiguration leading to missed alerts

Module 3: Threat Intelligence & Detection Techniques

- Types and sources of threat intelligence
- Integrating intelligence feeds into SOC workflows
- Matching indicators of compromise with internal data
- Identifying threat patterns and early warning signals
- Using MITRE ATT&CK for detection mapping
- Case Study: Stopping an attack using actionable threat intelligence

Module 4: Network Traffic Monitoring & Analysis

- Basics of network protocols and traffic flows
- Packet capture and inspection techniques
- Identifying anomalies in network behavior
- Tools for network threat hunting and analysis
- Recognizing signs of lateral movement and data exfiltration
- Case Study: Detecting a stealthy command-and-control connection

Module 5: Endpoint Security & Incident Response

- Endpoint detection and response fundamentals
- Identifying malicious processes and system changes
- Containing compromised endpoints
- Forensic evidence collection procedures
- Documenting and reporting incident findings
- Case Study: Responding to a ransomware-infected workstation

Module 6: Cyberattack Techniques & Behavioral Analytics

- Understanding attacker methodologies and kill chains
- Detecting suspicious user activities and privilege abuse
- Analyzing patterns of brute-force and credential misuse
- Spotting indicators of insider threats
- Using analytics to identify abnormal system behavior
- Case Study: Behavioral anomaly leading to early breach detection

Module 7: Automation, SOAR & SOC Optimization

- Principles of SOC automation and orchestration
- Implementing SOAR workflows for faster response
- Automating alert triage and repetitive tasks
- Improving SOC efficiency through optimization
- Integrating automated enrichment processes
- Case Study: SOC transformation through SOAR deployment

Module 8: Reporting, Documentation & Continuous Improvement

- Preparing clear and actionable incident reports
- Communicating with technical and non-technical stakeholders
- Tracking lessons learned and recurring threat patterns
- Maintaining SOC documentation and procedural updates
- Implementing continuous improvement strategies
- Case Study: Organizational improvement from post-incident review

Training Methodology

- Instructor-led presentations and demonstrations
- Hands-on exercises using SOC investigation tools
- Realistic case studies and log analysis scenarios
- Group discussions and collaborative problem-solving

- Practical labs simulating threat detection workflows
- End-of-course assessment for skill validation

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/certified-soc-analyst-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.