CYBERSECURITY · SHORT COURSE

Cyber Security Analysis – Threats, Tools, Risk & Incident Response (Hands-on)

Organizations today deploy multiple security tools including:

DATES	23–27 Nov 2026	DURATION	5-day course
COURSE FEE	TZS 1,300,000 · per participant	VAT	Fee excludes VAT
VENUE	Arusha, Tanzania	DAILY HOURS	8:30 AM – 4:30 PM
FEE INCLUDES	Course materials, lunch and refreshments	CERTIFICATE	Certificate of attendance
TRAINER	Elly International training team	APPLICATIONS	Open for applications

Overview

Organizations today deploy multiple security tools including:

- Firewalls
- Endpoint protection systems
- Intrusion detection systems
- SIEM platforms
- Email security gateways

Despite having these tools, many ICT and security teams face challenges such as:

- Large volumes of alerts without clear prioritization
- Difficulty distinguishing false positives from real threats
- Limited log interpretation skills
- Weak risk assessment thinking
- Delayed or inconsistent incident response decisions
- Poor coordination during active security events

Security monitoring without analytical capability leads to alert fatigue, slow response, and increased impact during incidents.

There is therefore a strong need for a practical, hands-on course that strengthens threat analysis, log interpretation, risk evaluation, and structured incident response decision-making using realistic scenarios and industry-relevant tools.

Course content

Day 1: Threat Landscape & Analytical Foundations

Module 1: Modern Cyber Threats

- Malware, ransomware, phishing
- Insider threats
- Advanced persistent threats (APTs)
- MITRE ATT&CK framework overview

Module 2: Analytical Thinking in Cybersecurity

- Structured analysis techniques
- Hypothesis-based investigation
- Risk likelihood vs impact
- Threat prioritization models

Practical Session (Hands-On)

- Threat classification exercises
- Risk scoring workshop

Day 2: Log Interpretation & Alert Analysis

Module 3: Understanding Security Logs

- Firewall logs
- Endpoint logs
- Server logs
- Authentication logs

Module 4: Alert Investigation Techniques

- Identifying suspicious patterns
- Correlation of events
- IOC analysis
- Recognizing false positives

Practical Session (Hands-On)

- Log review scenarios
- Investigating simulated suspicious activity

Day 3: Risk Assessment & Decision-Making

Module 5: Risk-Based Response Planning

- Risk matrix development
- Severity classification
- Business impact analysis
- Prioritization of containment actions

Module 6: Threat Response Strategies

- Isolation vs monitoring decisions
- Blocking vs investigation balance
- Escalation procedures
- Coordination with management

Practical Session (Hands-On Labs)

- Incident decision-making simulations
- Risk assessment case studies

Day 4: Incident Response & Documentation

Module 7: Incident Response Lifecycle

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lessons learned

Module 8: Incident Reporting & Evidence Handling

- Timeline documentation

- Evidence preservation basics
- Reporting to management
- Communication protocols

Practical Session (Hands-On)

- Drafting a complete incident report
- Reviewing a flawed incident response case

Day 5: Tools Integration & Capstone Simulation

Module 9: Security Tools in Analysis

- SIEM basics
- Log aggregation
- Basic threat hunting concepts
- Dashboard interpretation

Module 10: Continuous Improvement & Maturity

- Metrics and KPIs for security teams
- Tabletop exercises
- Security posture improvement planning
- Team readiness assessment

Capstone Practical Simulation
Participants will complete a full threat analysis and response simulation including:

- Alert interpretation
- IOC identification
- Risk assessment
- Containment decision
- Documentation
- Management briefing

Course Wrap-Up

- Practical evaluation
- Participant reflections
- Facilitator recommendations
- Certificate guidance

Who should attend

Target Group

This course is suitable for:

- ICT Security Staff
- Security Analysts
- ICT Officers
- Risk and Compliance Staff
- System Administrators
- Network Administrators
- SOC Support Teams
- IT Operations Staff

Recommended Prerequisites

- Basic understanding of networking and IT systems
- Familiarity with security tools (helpful but not mandatory)
- No advanced cybersecurity certification required

How to apply

Apply online at elly.wysyntaxtest98.or.tz. Your place is confirmed only after we review your application and contact you, within 1 working day.

Apply for this course | Ask on WhatsApp | Email us

+255 757 066 880 · training@ellyinternational.co.tz · Boma Road, Arusha, Tanzania · P.O. Box 13424

Details correct as of 8 November 2026.