CYBERSECURITY · SHORT COURSE

Cyber Incident Response and Digital Forensics Readiness

This practical course equips ICT professionals, cybersecurity teams, system administrators, digital investigators, auditors, and incident response personnel with the knowledge and practical skills required to prepare for, detect, respond to, investigate, and recover from cybersecurity incidents.

DATES	4–8 Jan 2027	DURATION	5-day course
COURSE FEE	TZS 1,200,000 · 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

This practical course equips ICT professionals, cybersecurity teams, system administrators, digital investigators, auditors, and incident response personnel with the knowledge and practical skills required to prepare for, detect, respond to, investigate, and recover from cybersecurity incidents.

Participants will explore the complete cyber incident response lifecycle, including incident identification, triage, containment, eradication, recovery, evidence preservation, investigation, documentation, and post-incident improvement. The course introduces practical approaches for handling incidents such as malware infections, ransomware, phishing, unauthorized access, account compromise, data breaches, insider threats, and suspicious network activity.

The digital forensics component focuses on forensic readiness and the preservation, collection, examination, analysis, and documentation of digital evidence. Participants will learn how to establish appropriate procedures before an incident occurs, maintain evidence integrity and chain of custody, document investigative activities, and support investigations while minimizing the risk of evidence contamination.

Through practical demonstrations, incident simulations, case studies, forensic exercises, and guided investigations, participants will develop practical incident response and forensic readiness capabilities that can be applied within organizational, public-sector, corporate, and enterprise environments.

Course content

Module 1: Cybersecurity Incident Response Fundamentals

- Introduction to cyber incident response
- Cybersecurity incidents versus security events
- Common types of cyber incidents
- Malware and ransomware incidents
- Phishing and social engineering incidents
- Unauthorized access and account compromise

- Data breaches and information leakage
- Insider threats
- Denial-of-service and network attacks
- Roles and responsibilities of an incident response team
- Incident response policies and procedures

Module 2: Incident Response Lifecycle and Frameworks

- Incident response lifecycle
- Preparation
- Detection and analysis
- Containment
- Eradication
- Recovery
- Post-incident activities
- Incident severity classification
- Incident prioritization and escalation
- Developing incident response playbooks
- Communication and coordination during incidents
- Lessons learned and continuous improvement

Module 3: Incident Detection, Triage and Initial Analysis

- Identifying indicators of compromise
- Security alerts and event analysis
- Log analysis fundamentals
- Endpoint and network indicators
- User and system behaviour anomalies
- Incident validation and false-positive analysis
- Initial incident assessment
- Determining scope and severity
- Establishing an incident timeline
- Collecting initial evidence
- Documenting incident observations

Module 4: Incident Containment and Eradication

- Short-term and long-term containment
- Isolating compromised systems
- Account containment and credential protection
- Malware containment
- Network segmentation during incidents
- Blocking malicious connections and indicators
- Removing malware and persistence mechanisms
- Vulnerability remediation
- System restoration and hardening
- Preventing incident recurrence
- Practical containment scenarios

Module 5: Digital Forensics Fundamentals

- Introduction to digital forensics
- Principles of digital evidence
- Types of digital evidence

- Computer and endpoint forensics
- Network forensics
- Mobile device forensics
- Cloud and virtual environment forensics
- Email and web forensics
- File-system and operating-system artefacts
- Volatile versus non-volatile evidence
- Challenges in digital forensic investigations

Module 6: Forensic Readiness and Evidence Preservation

- Understanding forensic readiness
- Developing a forensic readiness strategy
- Identifying potential sources of digital evidence
- Evidence preservation principles
- Acquisition planning
- Maintaining evidence integrity
- Hashing and integrity verification
- Write protection and evidence handling
- Documentation and investigative records
- Chain of custody
- Legal, regulatory and organizational considerations

Module 7: Digital Evidence Collection and Acquisition

- Planning evidence collection
- Identifying relevant devices and systems
- Disk and storage acquisition concepts
- Memory acquisition concepts
- Log and event data collection
- Email evidence collection
- Browser and application artefacts
- Network traffic and packet evidence
- Cloud-based evidence considerations
- Evidence storage and secure handling
- Verifying collected evidence

Module 8: Forensic Examination and Analysis

- File-system analysis
- Deleted-file and artefact analysis
- Metadata examination
- Timeline analysis
- User activity reconstruction
- Browser and application history
- Email and communication artefacts
- Malware and suspicious-file analysis
- Log correlation and event reconstruction
- Identifying indicators of compromise
- Building an evidence-based incident timeline

Module 9: Network and Endpoint Incident Investigation

- Network security monitoring fundamentals

- Network traffic analysis
- IP addresses, ports and protocols
- Identifying suspicious network activity
- Endpoint investigation techniques
- Windows and Linux forensic artefacts
- Authentication and access logs
- Persistence and privilege escalation indicators
- Detecting lateral movement
- Command execution and process analysis
- Correlating endpoint and network evidence

Module 10: Incident Reporting, Documentation and Communication

- Principles of incident documentation
- Maintaining an incident activity log
- Developing incident timelines
- Technical incident reports
- Executive incident reports
- Evidence-based findings
- Documenting investigative procedures
- Communicating incidents to management
- Internal and external incident notification
- Recommendations and corrective actions
- Preparing reports for audit, compliance, and legal processes

Module 11: Cyber Incident Recovery and Post-Incident Improvement

- System recovery and restoration
- Validating system integrity after recovery
- Password and credential resets
- Vulnerability remediation
- Security control improvement
- Monitoring systems after recovery
- Root-cause analysis
- Lessons-learned meetings
- Updating incident response procedures
- Improving forensic readiness
- Developing preventive and corrective action plans

Module 12: Practical Cyber Incident Response and Digital Forensics Simulation

- Developing an organizational incident response plan
- Incident identification and triage exercise
- Phishing and compromised-account investigation
- Malware and ransomware incident simulation
- Endpoint evidence collection exercise
- Log and timeline analysis
- Network evidence investigation
- Evidence integrity and chain-of-custody exercise
- Incident containment and recovery simulation
- Preparation of a forensic investigation report
- Executive incident briefing
- Development of an institutional incident response improvement plan

Who should attend

This course is designed for:

- Cybersecurity professionals
- ICT officers and managers
- Security operations centre (SOC) personnel
- Incident response team members
- Digital forensic investigators
- System and network administrators
- IT auditors
- Information security officers
- Cybersecurity analysts
- Network security professionals
- Database and systems administrators
- Risk and compliance officers
- Internal auditors
- Data protection and privacy professionals
- Law enforcement and investigative personnel
- ICT managers and technology leaders
- Government and public-sector ICT professionals
- Professionals responsible for cybersecurity incident management

Suitable Sectors

The course is particularly relevant to government ministries, departments and agencies, local government authorities, public institutions, banks and financial institutions, telecommunications companies, universities and educational institutions, healthcare organizations, insurance companies, technology companies, critical infrastructure operators, NGOs, development organizations, law enforcement and investigative institutions, and private organizations that manage sensitive information and digital systems.

How to apply

Apply online at ellyinternational.co.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 28 November 2026.