



ECIH Cybersecurity Incident Handling Practice Training Course

27 June – 1 July 2027
Nairobi

ECIH Cybersecurity Incident Handling Practice Training Course

Ref: 752_157261 **Date:** 27 June – 1 July 2027 **Location:** Nairobi **Fees:** 6000 Euro

Overview

ECIH Cybersecurity Incident Handling Practice Training Course is a five-day intermediate course for security operations analysts, incident responders, IT administrators, network defenders, forensic support staff, and risk professionals who leave with an Incident Handling and Recovery Playbook. Participants connect preparation, detection, validation, scoping, containment, evidence preservation, eradication, recovery, communication, reporting, and improvement through scenario-based decisions. Agile Leaders Training Center develops ECIH cybersecurity incident handling practice.

Who Should Attend

- Security operations functions responsible for alert validation, triage, and escalation
- Incident response functions responsible for coordinating technical and business actions
- Technology administration functions responsible for affected systems, networks, accounts, and restoration
- Forensic support functions responsible for preserving and transferring incident evidence
- Risk and continuity functions responsible for impact, communication, and recovery coordination

The course assumes participants work with security alerts, system or network evidence, operational procedures, or recovery activities, and leaves out malware development, offensive exploitation, forensic laboratory acquisition, certification preparation, and exam coaching.

Departments and Industries

The course supports departments and industries that require coordinated cybersecurity incident handling.

- Security operations and cyber defense
- IT infrastructure and service management
- Risk, continuity, and crisis coordination
- Financial services and healthcare
- Telecommunications, industrial operations, and digital services

Learning Objectives

By the end of this course, participants will be able to:



- Apply NIST SP 800-61 Rev. 3 recommendations to incident handling
- Analyze alerts, evidence, scope, severity, and business impact
- Build containment, evidence-preservation, and communication actions
- Evaluate eradication and recovery readiness
- Prioritize reporting, handovers, and stakeholder updates
- Build an Incident Handling and Recovery Playbook

Course Agenda

Day 1: Prepare Incident Handling

- NIST SP 800-61 Rev. 3 Response Outcome Map
- Incident Handling Roles and Authority Matrix
- Service, Asset, and Dependency Context Sheet
- Incident Communication and Escalation Directory
- Response Readiness and Evidence Source Checklist

Day 2: Detect, Validate, and Scope

- Alert Validation and Confidence Decision Tree
- Incident Classification and Severity Matrix
- Event Timeline and Correlation Worksheet
- Affected Asset and Account Scope Register
- Incident Impact and Priority Assessment

Day 3: Contain and Preserve Evidence

- Short-Term and Sustained Containment Planner
- Network, Endpoint, and Identity Action Board
- Volatile and Retained Evidence Priority Guide
- Evidence Handling and Transfer Record
- Containment Validation and Re-Scoping Checklist

Day 4: Eradicate, Recover, and Learn

- Root Cause and Persistence Removal Plan
- System Restoration and Dependency Sequence Map
- Recovery Validation and Monitoring Record
- Incident Status and Management Report
- Post-Incident Learning and Improvement Register



Day 5: Practice Incident Handling

- Exercise: Validate Alerts and Define Incident Scope
- Exercise: Select Containment and Evidence Actions
- Exercise: Coordinate Eradication and Restoration
- Exercise: Deliver Status, Handover, and Lessons Learned
- Capstone: Incident Handling and Recovery Playbook

Practical Exercises

The course uses suggested activities based on financial services, healthcare, telecommunications, industrial operations, and digital services.

- Suggested activity: validate alerts, build an event timeline, and record affected assets, accounts, and business services.
- Suggested activity: choose containment actions while preserving volatile and retained evidence for authorized review.
- Suggested activity: sequence eradication, restoration, validation, monitoring, and stakeholder communication.
- Suggested activity: produce a management report and improvement register from an incident scenario.

FAQs

Who suits ECIH cybersecurity incident handling training, and what does it assume?

Security operations, response, IT administration, network defense, forensic support, risk, and continuity functions suit the course; it assumes work with alerts, evidence, procedures, or recovery activities.

How does ECIH incident handling training differ from digital forensics training?

ECIH incident handling training coordinates decisions from detection through recovery, while digital forensics training concentrates on specialized acquisition, examination, and interpretation of digital evidence.

How does NIST SP 800-61 Rev. 3 support incident handling?

NIST SP 800-61 Rev. 3 integrates incident response considerations across cybersecurity risk management, connecting preparation, detection, response, recovery, and improvement outcomes.

How should incident handlers choose containment actions?

Incident handlers should compare urgency, affected services, attacker activity, evidence risk, operational impact, available isolation options, and the possibility of re-scoping before selecting containment actions.



What belongs in an Incident Handling and Recovery Playbook?

An Incident Handling and Recovery Playbook contains roles, evidence sources, classification criteria, timelines, scope records, containment choices, evidence controls, eradication and recovery actions, communications, reports, and improvement owners.

Conclusion

Participants take back an Incident Handling and Recovery Playbook that organizes decisions, evidence, actions, and communications. It changes fragmented reaction into a traceable path from validation and scoping through containment, recovery, and learning. The playbook supports timely coordination, defensible handovers, service restoration, and improvement after incidents.