



C|CT Cybersecurity Technician Foundation Skills Training Course

8 – 12 March 2027
Kuala Lumpur

C|CT Cybersecurity Technician Foundation Skills Training Course

Ref: 751_157182 **Date:** 8 – 12 March 2027 **Location:** Kuala Lumpur **Fees:** 6500 Euro

Overview

C|CT Cybersecurity Technician Foundation Skills Training Course is a five-day foundation course for entry-level technicians, IT support staff, junior analysts, network administrators, and career changers who leave with a Technician Security Operations Workbook. Participants build cybersecurity technician skills through system and network mapping, account review, secure configuration, vulnerability recording, traffic and log triage, incident tickets, and recovery checks. Agile Leaders Training Center develops foundation cybersecurity technician practice.

Who Should Attend

- Technology support functions responsible for maintaining user devices and resolving access issues
- Network administration functions responsible for connectivity, configuration, and traffic visibility
- Junior security functions responsible for monitoring events and escalating suspicious activity
- System operations functions responsible for accounts, services, updates, and backups
- Career-entry learners preparing to perform supervised cybersecurity tasks

The course assumes participants can navigate common operating systems and basic networks, and leaves out advanced exploitation, malware development, forensic acquisition, certification preparation, and exam coaching.

Departments and Industries

The course supports departments and industries that need consistent foundation security tasks.

- IT support and service operations
- Network and system administration
- Security operations and incident support
- Financial services and healthcare
- Retail, logistics, and digital services

Learning Objectives

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



- Apply technician task and escalation boundaries
- Build system, network, account, and data maps
- Use secure configuration and access review checklists
- Analyze vulnerability, traffic, and log evidence
- Prioritize incident tickets and containment support
- Evaluate recovery checks and technician handovers

Course Agenda

Day 1: Establish Technician Foundations

- NICE Framework Task, Knowledge, and Skill Map
- Cybersecurity Technician Responsibility and Escalation Matrix
- Asset, Service, and Data Inventory Worksheet
- Network Topology and Trust Boundary Diagram
- Operating System Account and Service Baseline

Day 2: Protect Systems and Access

- User Account Lifecycle Review Checklist
- Privilege Assignment and Access Exception Register
- Endpoint Secure Configuration Verification Sheet
- Patch and Update Status Tracking Board
- Backup Protection and Restoration Readiness Record

Day 3: Record Vulnerabilities and Network Evidence

- Vulnerability Finding Validation Worksheet
- Exposure and Remediation Priority Grid
- Packet Flow and Protocol Observation Guide
- Firewall Rule Review and Change Record
- Network Anomaly Evidence Capture Log

Day 4: Triage Logs and Incidents

- Security Log Source Coverage Matrix
- Authentication and Administrative Event Review
- Alert Triage and Confidence Decision Tree
- Incident Ticket Classification and Escalation Form
- Containment Support and Evidence Handling Checklist



Day 5: Practice Technician Operations

- Exercise: Map Assets, Accounts, and Network Boundaries
- Exercise: Verify Endpoint and Access Configurations
- Exercise: Rank Vulnerabilities and Network Anomalies
- Exercise: Triage Logs and Prepare an Incident Handover
- Capstone: Technician Security Operations Workbook

Practical Exercises

The course uses suggested activities based on healthcare, financial services, retail, logistics, and digital-service environments.

- Suggested activity: map a service, its devices, accounts, data, network paths, and escalation owners.
- Suggested activity: verify endpoint settings, privileges, updates, and backup readiness against technician checklists.
- Suggested activity: analyze vulnerability records, packet observations, authentication logs, and administrative events.
- Suggested activity: classify an incident ticket, record containment support, and prepare a recovery handover.

FAQs

Who suits C | CT cybersecurity technician foundation training, and what does it assume?

Entry-level technicians, support staff, junior analysts, network administrators, and career changers suit the course; it assumes basic operating-system and network navigation.

How does cybersecurity technician training differ from penetration testing training?

Cybersecurity technician training develops supervised defensive operations, evidence handling, and escalation skills, while penetration testing training focuses on authorized weakness discovery and exploitation methods.

How do cybersecurity technicians use logs for incident triage?

Cybersecurity technicians compare authentication, administrative, network, application, and system events, identify deviations, record evidence, assign confidence, and escalate according to defined criteria.

How should cybersecurity technicians prioritize vulnerability findings?

Cybersecurity technicians combine affected assets, exposure, observed exploitation, business importance, available remediation, and validation evidence to support prioritization.



What belongs in a Technician Security Operations Workbook?

A Technician Security Operations Workbook contains asset maps, account reviews, configuration checks, vulnerability records, traffic observations, log decisions, incident tickets, recovery checks, and handover notes.

Conclusion

Participants take back a Technician Security Operations Workbook that organizes foundation tasks and evidence. It changes informal troubleshooting into traceable protection, observation, triage, escalation, and recovery support. The workbook helps technicians apply consistent checks, document decisions, and hand work to specialist teams with usable context.