



# **Network Defense Operations and Incident Response Training Course**

26 – 30 April 2027  
Tbilisi

## Network Defense Operations and Incident Response Training Course

**Ref:** 1660\_222642 **Date:** 26 – 30 April 2027 **Location:** Tbilisi **Fees:** 5000 Euro

### Overview

Network Defense Operations and Incident Response Training Course is a one-week course for network administrators, security operations analysts, infrastructure engineers and IT support teams, who leave with a Network Defense Operations Pack. It connects secure network architecture, firewall policy, network segmentation, traffic monitoring, intrusion detection and incident response through operating evidence. Participants build a traceable defense workflow. Agile Leaders Training Center develops practical network defense operations capability.

### Who Should Attend

- Network teams responsible for architecture, connectivity and traffic controls
- Security operations teams responsible for detection, triage and response
- Infrastructure teams responsible for device configuration and hardening
- IT support teams responsible for endpoint and network issue escalation
- Risk teams responsible for vulnerability and control evidence
- Incident teams responsible for containment, recovery and lessons learned

The course assumes participants support enterprise networks or security operations, and it leaves out vendor-specific product administration, penetration testing and certification preparation.

### Departments and Industries

The course supports departments and industries that depend on connected systems and controlled network services.

- Network engineering, infrastructure and security operations
- Cybersecurity, technology risk and incident management
- Financial services, insurance and professional services
- Healthcare, education and public services
- Energy, manufacturing and industrial operations
- Retail, logistics and digital service providers

### Learning Objectives

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



- Build network asset and attack-surface maps
- Apply firewall, segmentation and hardening controls
- Analyze traffic, alerts and security logs
- Prioritize vulnerabilities and patch actions
- Diagnose network incidents and containment options
- Build response evidence and improvement plans

## **Course Agenda**

### **Day 1: Network Assets and Defense Architecture**

- Network Asset Inventory and Data Flow Map
- Attack Surface and Trust Boundary Diagram
- Defense-in-Depth Control Layer Model
- Administrative Access and Management Plane Matrix
- Network Defense Risk and Ownership Register

### **Day 2: Firewalls Segmentation and Hardening**

- NIST SP 800-41 Rev. 1 Firewall Policy Method
- Default-Deny Rule Base and Exception Log
- VLAN DMZ and Security Zone Design
- Network Device Hardening Checklist
- Configuration Baseline and Change Control Record

### **Day 3: Traffic Monitoring and Intrusion Detection**

- Traffic Visibility and Collection Point Plan
- Network Flow and Packet Analysis Worksheet
- Intrusion Detection Rule and Alert Matrix
- Security Log Source and Retention Map
- Alert Triage and Escalation Decision Tree

### **Day 4: Vulnerabilities Incidents and Recovery**

- Vulnerability Exposure and Patch Priority Matrix
- NIST SP 800-61 Rev. 3 Response Profile
- Network Incident Containment Playbook
- Evidence Timeline and Chain-of-Custody Log
- Recovery Validation and Improvement Register



## **Day 5: Network Defense Operations Practice**

- Exercise: Map an Exposed Network Service
- Exercise: Review Firewall and Segmentation Rules
- Exercise: Investigate Traffic and Detection Alerts
- Exercise: Contain and Recover a Network Incident
- Capstone: Network Defense Operations Pack

### **Practical Exercises**

Suggested activities use network diagrams, configuration records, traffic evidence, alerts and incident scenarios.

- Suggested activity: map assets, trust boundaries and management paths for a service environment
- Suggested activity: test firewall, segmentation and hardening decisions against required traffic flows
- Suggested activity: correlate network flow, packet and log evidence during alert triage
- Suggested activity: document containment, recovery and improvement actions in an operations pack

### **FAQs**

#### **Who should take network defense operations training, and what does it assume?**

It suits network, infrastructure, security operations, IT support and incident teams that already support enterprise networks or security controls.

#### **How does network defense operations training differ from general cybersecurity training?**

Network defense operations training concentrates on network architecture, traffic controls, monitoring, detection and incident handling; general cybersecurity training covers a wider range of people, process, application, data and technology risks.

#### **What does a network defense operating model include?**

A network defense operating model includes asset ownership, trust boundaries, traffic policy, hardening baselines, monitoring sources, alert decisions, vulnerability priorities, incident playbooks and evidence responsibilities.

#### **Why is network segmentation important for network defense?**

Network segmentation separates systems by purpose and risk, restricts unnecessary traffic paths, limits lateral movement and creates clearer monitoring and policy boundaries.



## **How do network monitoring and incident response work together?**

Network monitoring supplies flow, packet, alert and log evidence that supports incident detection, analysis, containment decisions, recovery validation and improvement.

### **Conclusion**

Participants take back a Network Defense Operations Pack containing architecture, firewall, segmentation, hardening, monitoring, vulnerability, incident and improvement artifacts. The pack connects network controls to evidence and decision paths. It helps teams operate defenses consistently, investigate alerts and document response actions.