Network Security Operations Management Training Course

5 – 9 April 2027
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Network Security Operations Management Training Course

Ref: 1696_227505 **Date:** 5 – 9 April 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Network Security Operations Management Training Course is a one-week professional course for IT operations managers, network leads, security coordinators, infrastructure managers, and service owners, who leave with a Network Security Operations Management Pack. It connects network security operations management, network asset inventory, secure network configuration, access, segmentation, network monitoring and logging, network incident response, resilience, suppliers, service levels, and governance. Agile Leaders Training Center presents the course on managing network reliability and cybersecurity.

Who Should Attend

- Teams responsible for network availability, configuration, and service performance
- Functions responsible for cybersecurity coordination and risk acceptance
- Leaders responsible for identity, access, segmentation, and administration
- Teams responsible for vulnerability, monitoring, incidents, and recovery
- Service owners responsible for suppliers, reporting, and governance

The course assumes participants coordinate IT services, networks, infrastructure, security, or operational risk and leaves out device configuration and security testing.

Departments and Industries

The course supports managers coordinating network operations and cybersecurity across service environments.

- Network, infrastructure, and IT operations departments
- Cybersecurity, risk, and security operations functions
- Service management and business continuity teams
- Banking and insurance technology operations
- Healthcare networks and information systems functions
- Energy and industrial infrastructure teams

Learning Objectives

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

- Build a network and security accountability model
- Analyze asset, topology, configuration, and dependency visibility
- Evaluate access, segmentation, vulnerability, and supplier controls
- Use monitoring and logging evidence to prioritize action
- Apply incident, recovery, and resilience coordination
- Build service, risk, and governance measures

Course Agenda

Day 1: Operating Model and Visibility

- Network and Security Operating Model and RACI Matrix
- Network Asset Inventory and Ownership Register
- Network Topology, Zone, and Dependency Map
- Service Criticality and Business Impact Classification
- NIST Cybersecurity Framework 2.0 Profile

Day 2: Configuration, Access, and Segmentation

- Secure Network Configuration Baseline and Exception Log
- Change and Configuration Evidence Chain
- Identity, Device, and Privileged Access Matrix
- NIST SP 800-207 Zero Trust Policy Model
- Network Segmentation and Trust Boundary Review

Day 3: Exposure, Monitoring, and Suppliers

- Vulnerability Exposure and Remediation Matrix
- Network Monitoring Use Case and Alert Catalog
- Log Source Coverage and Retention Map
- Supplier Remote Access Control Register
- Network Service and Security Measure Dashboard

Day 4: Incidents, Recovery, and Governance

- Network Incident Classification and Escalation Matrix
- Containment, Eradication, and Recovery Coordination
- Backup, Restore, Failover, and Recovery Evidence
- Network Resilience Scenario Analysis
- Risk Acceptance and Governance Review Pack

Day 5: Network Security Management Practice

- Asset, Topology, and Criticality Mapping Exercise
- Configuration, Access, and Segmentation Exercise
- Monitoring, Vulnerability, and Supplier Exercise
- Incident, Recovery, and Resilience Exercise
- Network Security Operations Management Pack Capstone Exercise

Practical Exercises

The course uses suggested activities to practice management decisions without device configuration.

- Suggested activity: reconcile asset, topology, ownership, dependency, and criticality data.
- Suggested activity: review an access path and segmentation change against zero-trust questions.
- Suggested activity: prioritize vulnerability and monitoring gaps using impact and exposure.
- Suggested activity: coordinate containment, continuity, recovery, communication, and governance.

FAQs

Who suits network security operations management training and what does it assume?

Network security operations management training suits professionals coordinating networks, infrastructure, security, services, or operational risk. It assumes workplace exposure to IT operations and does not teach device commands.

How does network security operations management differ from network engineering training?

Network security operations management focuses on accountability, risk, evidence, access, segmentation, monitoring, incidents, resilience, suppliers, and governance. Network engineering training focuses on network design and configuration.

Why is a network asset inventory important for security operations?

A network asset inventory identifies devices, owners, locations, dependencies, service relationships, and criticality. It supports configuration, vulnerability, monitoring, incident, and lifecycle decisions.

How does network monitoring and logging support management decisions?

Network monitoring and logging provide evidence about availability, access, changes, anomalous activity, control coverage, incidents, and supplier behavior. Managers use defined use cases and impact to prioritize action.

AGILE LEADERS
Training Center

What should a network incident response process coordinate?

A network incident response process coordinates classification, ownership, escalation, containment, evidence, communication, continuity, recovery, supplier action, lessons, and risk decisions.

Conclusion

Participants take a Network Security Operations Management Pack back to work. It connects assets, topology, configuration, access, segmentation, vulnerability, monitoring, incidents, recovery, suppliers, measures, and governance. It changes fragmented activity into accountable evidence for reliability, risk, resilience, escalation, and investment decisions.