Advanced Enterprise Network Defence Training Course

19 – 23 September 2027
Cape town

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Advanced Enterprise Network Defence Training Course

Ref: 1651_221978 **Date:** 19 – 23 September 2027 **Location:** Cape town **Fees:** 4500 Euro

Overview

Advanced Enterprise Network Defence Training Course is a one-week professional programme for network security, SOC, incident response, infrastructure, and security-engineering practitioners, who leave with a Network Defence Improvement Plan. It addresses gaps between architecture, telemetry, detection, hunting, and response through trust-zone analysis, secure device management, traffic evidence, threat-informed detection, authorised validation, and measured improvement across hybrid environments. Agile Leaders Training Center develops practical advanced enterprise network defence capability.

Who Should Attend

- Network-security teams responsible for defensive architecture and controls
- SOC teams responsible for network monitoring and investigation
- Incident-response functions responsible for containment and evidence
- Infrastructure teams responsible for secure network-device operation
- Detection engineers responsible for analytics and coverage
- Security-assurance teams responsible for validating defensive effectiveness

The course assumes participants can interpret network protocols, addressing, routing, security controls, and logs and leaves out offensive activity against third-party or production systems.

Departments and Industries

The course supports organisations that operate business-critical networks across on-premises, cloud, remote, and partner environments.

- Cybersecurity operations, engineering, architecture, and incident response
- Network, infrastructure, cloud, and platform operations
- Banking, insurance, telecommunications, and technology
- Energy, utilities, manufacturing, and logistics
- Healthcare, education, retail, and professional services
- Governance, risk, assurance, and managed security services

Learning Objectives

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

- Analyze assets, trust zones, flows, dependencies, and attack paths
- Build segmentation and identity-aware network controls
- Use packet, flow, DNS, proxy, firewall, and device telemetry
- Apply network detection engineering and threat hunting
- Diagnose intrusions and prioritize containment actions
- Evaluate defensive coverage through authorised validation

Course Agenda

Day 1: Defence Architecture and Exposure

- NIST CSF 2.0 Outcomes for Network Defence
- Assets, Services, Dependencies, and Data Flows
- Trust Zones, Boundaries, and Attack Paths
- Network Device and Management-Plane Security
- Current-State Network Defence Map

Day 2: Segmentation and Zero Trust

- Segmentation, Segregation, and Policy Enforcement
- Zero Trust Network Defence Principles
- Identity, Device Posture, and Resource Access
- Remote, Cloud, Partner, and Administrative Paths
- Control Architecture and Exception Review

Day 3: Telemetry and Detection Engineering

- Packet, Flow, DNS, Proxy, Firewall, and Device Logs
- Telemetry Quality, Time, Context, and Retention
- MITRE ATT&CK Network Device Techniques
- Network Detection Engineering and Analytic Logic
- Coverage Map, Test Data, and Tuning

Day 4: Threat Hunting and Response

- Enterprise Network Threat Hunting Hypotheses
- Traffic Baselines, Anomalies, and Encrypted Channels
- Credential Access, Discovery, and Lateral Movement
- Command-and-Control, Exfiltration, and Impact
- Containment, Evidence, Recovery, and Escalation

AGILE LEADERS
Training Center

Day 5: Validation and Capstone

- Authorised Adversary Emulation and Safety Controls
- Purple-Team Scenarios and Detection Validation
- Control Effectiveness, Gaps, and Risk Priorities
- Metrics, Governance, and Improvement Backlog
- Capstone: Network Defence Improvement Plan

Practical Exercises

Suggested activities use authorised lab evidence to connect architecture, detection, and response.

- Suggested activity: map trust zones, critical flows, and plausible attack paths
- Suggested activity: analyse packet and flow evidence for a network intrusion scenario
- Suggested activity: write and tune a threat-informed network detection analytic
- Suggested activity: validate detection and containment through a controlled purple-team exercise

FAQs

Who should take advanced enterprise network defence training, and what does it assume?

It suits experienced network, SOC, response, infrastructure, detection, and assurance practitioners and assumes working knowledge of protocols, routing, access controls, and logs rather than beginner-level networking.

How does advanced enterprise network defence differ from a general cybersecurity course?

Advanced network defence concentrates on enterprise flows, trust boundaries, network-device security, telemetry, detection logic, threat hunting, intrusion response, and validation. General cybersecurity courses usually span a broader range of governance, identity, endpoint, application, data, and awareness topics.

Does zero trust network defence eliminate segmentation?

No. Zero trust removes implicit trust based on location and protects resources through continuous, contextual access decisions. Segmentation can still reduce exposure and enforce communication policy when designed around resources, identities, workloads, and verified requirements.

How does threat-informed network defence use MITRE ATT&CK?

Defenders use ATT&CK as a common language to identify relevant adversary behaviours, map telemetry and analytic coverage, design hunting hypotheses, test detections, reveal gaps, and prioritise improvements without treating the matrix as a complete threat model.

Does advanced network defence training authorise testing external systems?

No. All exercises require explicit authorisation, defined scope, isolated or approved environments, safety controls, evidence handling, and stop conditions. The course provides no CAST certification, third-party endorsement, or permission to target systems.

Conclusion

Participants take back a Network Defence Improvement Plan linking critical flows, trust zones, segmentation, device security, telemetry, ATT&CK-informed coverage, detection analytics, hunting, containment, validation, metrics, and governance. It makes defensive assumptions and gaps visible. The plan helps teams prioritise improvements and test whether controls produce usable evidence against relevant network threats.