Infrastructure Security: First Line of Defense

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

System administrators, information technology operations staff, network administrators.

Training objectives

- Harden servers, workstations and networks.
- Implement effective patch and access management.
- Detect threats through logging and monitoring.
- Respond to incidents effectively.

Summary

This course covers IT infrastructure hardening, patch management, access, and incident response.

You will learn how to protect the infrastructure, the first line of defense against cyberattacks.

Course outline

Module 1: Infrastructure Security Fundamentals

- Threat Landscape for System Administrators.
- Defence in depth.
- Role of infrastructure in resilience.

Module 2: Hardening of Systems and Networks

- Patch and Vulnerability Management.
- Network and firewall segmentation.
- Identity and access management.

Module 3: Monitoring and Detection

- Logging and SIEM basics.
-

© 2026

IDS/IPS and monitoring tools.

Module 4: Incident Response for Administrators

- Key steps in incident response.
- Containment, eradication, recovery.
- Communication and escalation.

Approach and methodology

Curing guides and tool documentation provided.

Prerequisites

- Experience in managing Windows or Linux systems.
- Basic knowledge of networks.

Recommendations

- Basic understanding of IT infrastructures (servers, networks, systems)
- Notions of networking (IP, firewall, segmentation)
- Knowledge of cybersecurity concepts (common threats, best practices)
- Comfortable with Windows and/or Linux environments
- Sensitivity to the issues of protection, availability and integrity of systems

© 2026