# Sécurité de l'infrastructure: première ligne de défense

Durée: 1 jour
Public cible: Professionnel TI

## À qui s'adresse cette formation ?

Administrateurs systèmes, personnel d'exploitation technologies de l'information, administrateurs réseaux.

## Objectifs de la formation

- Durcir serveurs, postes et réseaux.
- Mettre en œuvre une gestion efficace des correctifs et des accès.
- Détecter les menaces par la journalisation et le monitoring.
- Répondre aux incidents efficacement.

## Description sommaire

Cette formation couvre le renforcement des infrastructures technologies de l'information, la gestion des correctifs, les accès et la réponse aux incidents. Vous apprendrez à protéger l'infrastructure, première ligne de défense contre les cyberattaques.

## Contenu du plan de cours

### Module 1 : Principes fondamentaux de la sécurité d'infrastructure

- Paysage des menaces pour les administrateurs systèmes.
- Défense en profondeur.
- Rôle de l'infrastructure dans la résilience.

### Module 2 : Durcissement des systèmes et réseaux

- Gestion des correctifs et vulnérabilités.
- Segmentation réseau et pare-feu.
- Gestion des identités et accès.

**Module 3 : Surveillance et détection**

- Journalisation et bases SIEM.
- IDS/IPS et outils de monitoring.

**Module 4 : Réponse aux incidents pour administrateurs**

- Étapes clés d'une réponse aux incidents.
- Confinement, éradication, récupération.
- Communication et escalade.

## Approche et méthode pédagogique

Guides de durcissement et documentation d'outils fournis.

## Prérequis

- Expérience en gestion de systèmes Windows ou Linux.
- Connaissances de base en réseaux.

## Recommandations

- Compréhension de base des infrastructures TI (serveurs, réseaux, systèmes)
- Notions en réseautique (IP, pare-feu, segmentation)
- Connaissance des concepts de cybersécurité (menaces courantes, bonnes pratiques)
- Aisance avec des environnements Windows et/ou Linux
- Sensibilité aux enjeux de protection, disponibilité et intégrité des systèmes