

Formation Sécurité systèmes et réseaux

Durée :	5 jours
Public :	Tous
Pré-requis :	Connaissance des protocoles réseaux
Objectifs :	Comprendre les enjeux de la sécurité d'un réseau informatique et savoir la mettre en œuvre
Référence :	Ré445-F
Demandeurs d'emploi :	Contactez-nous pour connaître les remises Pôle Emploi

Introduction

- Enjeux de la sécurité
- Évaluation des risques
- Critères de sécurité
- Normes liées à la sécurité
- Plans de continuité ou de reprise d'activité

Analyse du risque et des menaces

- Analyse des risques et élaboration des scénarios
- Caractérisation des menaces (sources, vulnérabilités, objectif)
- Savoir faire un inventaire des menaces caractéristiques
- Adéquation risque-menace et disponibilité

Atelier pratique : élaboration d'un scénario de risque, caractérisation de quelques menaces courantes

Les différents niveaux de gestion de la sécurité

- Sécuriser les données, les échanges, et le réseau
- Sécurité du système d'exploitation, réduction de la surface d'attaque
- Sécurité des applications
- Gestion des identités
- Auditer un système

Sécurité des données

- Les problématiques de l'accès physique
- Identification des ressources critiques
- Chiffrer les données

Sécurité des échanges de données

- Contraintes de sécurité : intégrité, confidentialité, non-répudiation
- Principes de chiffrement, symétrique, asymétrique (clés privées, secret partagé..)
- Contraintes liées au support (espionnage, liaisons sans fil..)

Sécurisation de Linux

- Permissions standards et étendues
- Gestion des profils de sécurité et des limitations des applications
- Utilisation de PAM
- Mise en place du pare-feu sur Linux
- Manipulation du chiffrement disque sur Linux
- Gestion des intrusions et des journaux (logs)

Sécurisation de Windows

- Gestion des droits
- Gestion des services
- Accès problématiques pour le réseau et les périphériques
- Configuration du pare-feu, et réflexions
- Possibilités de chiffrement
- Gestion du journal d'évènement et des audits

Audit d'un système

- Analyse externe au niveau réseau
- Inventaire des risques opérationnels
- Vérification du cloisonnement applicatif et utilisateur
- Risques liées à la maintenance du système (versions des logiciels, mauvaises configurations)
- Tentatives d'intrusion ciblées