

Réf : T130-070

Durée : 3 jours

Public

Responsables informatique, responsables systèmes, ingénieurs réseaux. Toute personne ayant en charge un système d'information d'entreprise.

Vous serez capable de

Connaitre les enjeux de la sécurité des SI à travers les dernières études en cybercriminalité.
Aborder les différents thèmes et besoins des entreprises en matière de sécurité
Aborder la sécurisation des systèmes d'information par l'analyse des risques
Définir les principes d'architecture de sécurité et l'état de l'art en matière de sécurisation du SI et des postes client.

Pré-requis

CONTENU PEDAGOGIQUE

Introduction & enjeux sécurité

Principes généraux de sécurité

Les services de sécurité

L'analyse et l'évaluation

Méthode EBIOS

SMSI ISO-27001 : 2005

Les biens, menaces, vulnérabilité et impacts

Audits de sécurité

Tableaux de bords sécurité

Les mesures de sécurité

La continuité d'activité

Les aspects juridiques

Les différents acteurs

Les attaques types, sur utilisateur et sur le poste de travail

La protection du poste client

La défense en profondeur

Le cloisonnement réseaux

Les architectures sécurisées

La DMZ et les filtrages

Le réseau local

VPN

IPSEC

La cryptographie

Les PKIs

La sécurisation de l'authentification

Conclusion