

## SOLUTION DE HAUTE DISPONIBILITÉ

Réf. : **SO32** Sécurité maximale des systèmes et réseaux Informatiques

Générique



Support de cours :  Certification : Nous consulter

Ce cours a pour objectif de fournir aux informaticiens les compétences et connaissances requises pour déployer et gérer les pare-feu et serveurs de mise en cache.

### PRE-REQUIS

- ☞ Connaissances de base des concepts de la sécurité
- ☞ Connaissances fondamentales du rôle d'un administrateur de sécurité.

### PARTICIPANTS

Ce cours s'adresse aux informaticiens Administrateurs Web, Administrateurs réseau et Administrateurs de sécurité.

### CONTENU DU COURS

- Module 1** : Introduction à la conception de la sécurité
- Module 2** : Création d'un plan pour la sécurité du réseau
- Module 3** : Identification des menaces pour la sécurité des réseaux
- Module 4** : Analyse du risque de la sécurité
- Module 5** : La boîte à outils du défenseur
- Module 6** : Missile virtuel de destruction massive
- Module 7** : Création d'un design de sécurité pour les ressources physiques
- Module 8** : Création d'un design de sécurité pour les ordinateurs
- Module 9** : Création d'un design de sécurité pour les périmètres réseau
- Module 10** : Détection de l'Intrusion Host
- Module 11** : Détection de l'Intrusion Réseau
- Module 12** : Outils de Scan
- Module 13** : Password Cracking
- Module 14** : Sauvegardes Légales
- Module 15** : Dénie de Service et Attaques de Déception
- Module 16** : Sécurité du Web
- Module 17** : Conversions de base, Adressage IP et Sous-réseaux
- Module 18** : Communications sécurisées
- Module 19** : Présentation & Architecture des Firewalls
- Module 20** : Implémentation & Déploiement des Firewalls
- Module 21** : Les réseaux VPN
- Module 22** : Surveillance et création de rapports (Logging)
- Module 23** : Les Personnels Firewall

Réf. : **SO35** Audit du système informatique

Générique



Support de cours :  Certification : Nous consulter

Les systèmes d'informations deviennent de plus en plus confrontés aux menaces de sécurité provenant de sources très variées, parmi lesquelles la fraude informatique, l'espionnage, le sabotage et le vandalisme, l'incendie ou l'inondation.

C'est dans ce contexte que nous avons mis en place un module de formation couvre les détails de mise en œuvre des principales phases de l'audit sécurité :

- ☞ l'audit des aspects organisationnels et physiques
- ☞ audit technique

### PRE-REQUIS

Pour suivre ce séminaire, les stagiaires doivent avoir une connaissance pratique des éléments suivants :

- ☞ Outils d'administration de Windows 2000 ou de Windows Server 2003 ;
- ☞ Active Directory et la stratégie de groupe.

### PARTICIPANTS

Les participants sont des administrateurs système ou réseau qui possèdent déjà de l'expérience dans Microsoft Windows 2000 Server ou Microsoft Windows Server™ 2003, et qui connaissent les concepts d'Active Directory®. Dans leurs entreprises, ils sont responsables de la gestion de la sécurité et des déploiements associés à leur infrastructure réseau interne, et à des services Internet ou intranet.

### CONTENU DU COURS

- Module 1** : Introduction à l'Audit Sécurité
- Module 2** : Audit Organisationnel & Physique (AOP)
- Module 3** : Audit Technique (AT)

Hors Déjeuner 900 DT ht 5 jours



2 jours 530 DT ht Hors Déjeuner

L'ensemble de nos formations sont adaptables en intra. Notre équipe est à votre disposition pour étudier avec vous la solution de formation la plus adaptée, contactez-nous Service Client n° 71 96 99 09

\*Toutes les marques citées sont déposées par leurs propriétaires respectifs