CONTENU DU COURS (5 jours) conseillés

Introduction à la sécurité de Windows Server

- Panorama des paramètres de sécurité
- Identification des principales catégories d'attaques
- Evaluation des failles de sécurité

Installation et optimisation d'un environnement de certificat de services

Administration de composants PKI

- Installation et configuration du serveur de certificats
- Création, révocation et suppression des certificats numériques

Détail des architectures d'authentification

- Etude des composants d'authentification
- Amélioration de l'authentification grâce aux stratégies de groupes
- Analyse de l'interaction avec Kerberos
- Mise à l'épreuve des failles

Déploiement d'un modèle de sécurité évolutif avec l'Active directory

Outils de contrôle et de déploiement de la sécurité

- Configuration et analyse de la sécurité
- Stratégies de groupes
- Modèles de sécurité

Repérage des failles dans votre système d'exploitation

- Verrouillage des services
- Identification des failles des applications
- Mise en place de nouvelles stratégies de restriction de logiciels
- Administration d'une stratégie de contrôle de la sécurité

Mesure des performances

Collecte des données

- Utilisation de processeurs et de la mémoire
- E/S disque et réseau

Etablir un jeu de références en utilisant le moniteur système

- Création de consoles de performances
- Configurer les alertes de performances

Dépannage avancé du système d'exploitation

- Maintenance des pilotes du système
- Dépannage du processus de démarrage
- Identification des causes de vidage de mémoire
- Faire face aux écrans bleus de démarrage

Gestion de l'intégrité du registre

- Réglage du registre
- Restauration des composants du registre

POUR QUI ?

Ce cours s'adresse à un public informaticien averti qui souhaite mettre en place la sécurité pour Windows Server.

POUR QUOI ?

- **Mettre en place des composants de sécurité**
- **Développer des stratégies de sécurité**
- **Dépanner le système Windows Server**

SYSTEMES RESEAUX