

Concevoir la sécurité d'un réseau Microsoft

Infos Générales



Public visé : Ingénieurs systèmes et responsables sécurité.



Objectifs : A la fin de ce cours les stagiaires sauront : identifier les menaces portant sur la sécurité réseau, analyser les risques de sécurité, concevoir la sécurité des ressources physiques, des ordinateurs, des données, de la transmission de données, de l'authentification des utilisateurs. Concevoir un périmètre de sécurité (DMZ), concevoir des procédures de réponse aux incidents.



Pré requis : Public déjà familiarisé avec Windows 2003 ou bien Windows 2000.

infos pratiques

Référence

MS2830 (US) - MS2113 (FR)

Vos contacts

Christelle et Caroline

Certification

70-298

Formateur

MCSE

Support

Microsoft Officiel

Durée



Repas



Café



Module 1 : Introduction à la conception de la sécurité.

Réseaux Microsoft

Etude de cas : société pharmaceutique Contoso

Module 2 : Créer un plan pour la sécurité réseau.

Introduction aux politiques de sécurité

Définition d'un processus de conception des risques réseau

Création d'une équipe de conception de la sécurité

Module 3 : Identifier les menaces portant sur la sécurité réseau.

Introduction aux menaces sur la sécurité

Prévision des risques portant sur la sécurité réseau

Module 4 : Analyse des risques de sécurité.

Introduction à la gestion des risques

Création d'un plan de gestion des risques

Module 5 : Mise en oeuvre de la sécurité des ressources physiques.

Déterminer les menaces sur les ressources physiques

Analyser les risques sur les ressources physiques

Concevoir la sécurité pour les ressources physiques

Module 6 : Mise en oeuvre de la sécurité des ordinateurs.

Déterminer les menaces sur les ordinateurs

Analyser les risques sur les ordinateurs

Concevoir la sécurité pour les ordinateurs

Module 7 : Mise en oeuvre de la sécurité des comptes utilisateurs.

Déterminer les menaces sur les comptes utilisateurs

Analyser les risques sur les comptes utilisateurs

Concevoir la sécurité pour les comptes utilisateurs

Module 8 : Mise en oeuvre de la sécurité des authentifications.

Déterminer les menaces sur les authentifications

Analyser les risques sur les authentifications

Concevoir la sécurité pour les authentifications

Module 9 : Mise en oeuvre de la sécurité des données.

Déterminer les menaces sur les données

Analyser les risques sur les données

Concevoir la sécurité pour les données

Module 10 : Mise en oeuvre de la sécurité sur la transmission de données.

Déterminer les menaces sur les transmissions de données

Analyser les risques sur les transmissions de données

Concevoir la sécurité pour les transmissions de données

Module 11 : Mise en oeuvre de la sécurité des DMZ.

Déterminer les menaces sur les DMZ

Analyser les risques sur les DMZ

Concevoir la sécurité pour les DMZ

Module 12 : Concevoir des réponses aux incidents de sécurité.

Introduction à l'audit et à la réponse aux incidents

Concevoir une politique d'audit

Concevoir une procédure de réponse aux incidents