



## Public

Ce cours s'adresse à des ingénieurs système et des spécialistes en sécurité responsables de la mise en place de stratégies et procédures de sécurité dans une organisation. Les stagiaires doivent posséder une à trois années d'expérience en conception de solutions d'entreprise.

## Connaissances requises

Une bonne connaissance des technologies principales de Microsoft® Windows® 2000, telles que traitées dans le cours Microsoft Learning 2053 : Implémentation de Microsoft Windows 2000 Professionnel et Server

Une bonne connaissance de l'implémentation et des technologies réseau de Windows 2000, telles que traitées dans le cours Microsoft Learning 2172 : Implémentation d'une infrastructure réseau Microsoft Windows 2000 ;

Une bonne connaissance de l'implémentation et des technologies de service d'annuaire Windows 2000, telles que traitées dans le cours Microsoft Learning 2174 :

Implémentation et administration des services d'annuaire Microsoft Windows 2000.

## Durée

3 jours

## Moyens Pédagogiques

Alternance de cours théoriques et d'exercices pratiques.

Une personne par poste micro.  
Support de cours.

## Modalités de suivi :

- Validation des compétences acquises par des exercices pratiques à la fin de chaque module.
- Test pratique reprenant l'intégralité des modules étudiés en fin de formation.
- A l'issue de la formation est remis un bilan stagiaire et une évaluation du formateur.
- Feuilles d'émargement.

## Animateur :

Consultant informaticien certifié MCT

## Contact commercial :

David DEHAIS

Tél : 02.35.590.591

Fax : 02.35.80.82.99

Email : d.dehais@aemy.fr

## Cours :

# MS 2113 Conception de la sécurité pour les réseaux Microsoft

## Objectif de la formation

Ce cours permet d'acquérir les connaissances et compétences nécessaires pour concevoir une infrastructure réseau sécurisée. Il aborde la mise en œuvre de l'équipe de conception, la modélisation des menaces et l'analyse des risques de sécurité afin de pouvoir répondre aux exigences de l'entreprise en matière de sécurisation des ordinateurs dans un environnement réseau. Ce cours fait appel aux compétences décisionnelles des participants grâce à un outil interactif qui simule des scénarios que les stagiaires seront susceptibles de rencontrer en situation réelle. Il est demandé de rassembler les informations et de trier les détails obtenus pour répondre aux exigences de sécurité.

## A l'issue de ce cours, les stagiaires seront capables de :

- planifier une structure pour la sécurité du réseau ;
- identifier les menaces pesant sur la sécurité du réseau ;
- analyser les risques de sécurité ;
- concevoir une sécurité pour les ressources physiques ;
- concevoir une sécurité pour les ordinateurs ;
- concevoir une sécurité pour les comptes ;
- concevoir une sécurité pour l'authentification ;
- concevoir une sécurité pour les données ;
- concevoir une sécurité pour la transmission des données ;
- concevoir une sécurité pour les périmètres des réseaux ;
- concevoir une procédure de réponse aux incidents.

## Annexes

- Conception d'une stratégie du bon usage
- Conception de stratégies de gestion des réseaux
- Conception d'une structure opérationnelle pour la gestion de la sécurité.

## Module 1 : Présentation de la conception de la sécurité

*Ce module décrit la structure de base utilisée pour la conception de la sécurité des réseaux et présente les concepts clés utilisés dans ce cours. Il présente également une étude de cas qui sera utilisée tout au long du cours, dans les travaux pratiques*

## Module 2 : Création d'un plan pour la sécurité du réseau

*Ce module traite de l'importance des stratégies et procédures de sécurité dans une conception de sécurité. Il explique également qu'une équipe de conception de la sécurité doit comprendre des membres représentant les divers postes de l'organisation.*





## Cours :

# MS 2113 Conception de la sécurité pour les réseaux Microsoft (suite)

### Compétences acquises :

- décrire les éléments courants des stratégies et procédures de sécurité ;
- créer une structure de conception de sécurité à l'aide du modèle de processus MSF ;

créer une équipe de conception de la sécurité

### Module 3 : Identification des menaces pesant sur la sécurité du réseau

*Ce module explique comment identifier les menaces potentielles qui pèsent sur un réseau, ainsi que les motivations des intrus. À la fin de ce module, vous serez à même d'expliquer les menaces courantes et prévoir les menaces à l'aide d'un modèle de menace.*

#### Compétences acquises :

- expliquer les vulnérabilités courantes des réseaux et comment les intrus peuvent les exploiter ;
- prédire les menaces sur la sécurité à l'aide du modèle STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege).

### Module 4 : Analyse des risques de sécurité

*Ce module explique comment déterminer les ressources, au sein d'une organisation, qui nécessitent une protection et comment les classer pour déterminer leur niveau de protection approprié. À la fin de ce module, vous serez à même d'appliquer une structure de planification de la gestion des risques.*

#### Compétences acquises :

- expliquer la finalité et le fonctionnement de la gestion des risques ;
- ébaucher les éléments d'un plan de gestion des risques.

### Module 5 : Création d'une conception de sécurité pour les ressources physiques

*Ce module décrit les menaces et risques pesant sur les ressources physiques d'une organisation et explique comment sécuriser les locaux, les ordinateurs et le matériel. À la fin de ce module, vous serez à même de concevoir la sécurité des ressources physiques.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques liés aux ressources physiques ;
- concevoir une sécurité pour les ressources physiques.

### Module 6 : Création d'une conception de sécurité pour les ordinateurs

*Ce module explique comment déterminer les menaces et analyser les risques pesant sur les ordinateurs de votre réseau. À la fin de ce module, vous serez à même de concevoir la sécurité pour les ordinateurs.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques pesant sur les ordinateurs ;
- concevoir une sécurité pour les ordinateurs.

### Module 7 : Création d'une conception de sécurité pour les comptes

*Ce module décrit les menaces et les risques pesant sur les comptes d'une organisation. À la fin de ce module, vous serez à même de concevoir la sécurité pour les comptes.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques pesant sur les comptes ;
- concevoir une sécurité pour les comptes.

### Module 8 : Création d'une conception de sécurité pour l'authentification

*Ce module décrit les menaces et les risques pesant sur l'authentification. À la fin de ce module vous serez à même de concevoir la sécurité pour l'authentification.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques pesant sur l'authentification ;
- concevoir une sécurité pour l'authentification.

### Module 9 : Création d'une conception de sécurité pour les données

*Ce module décrit les menaces et les risques pesant sur les données. À la fin de ce module vous serez à même de concevoir la sécurité pour les données.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques pesant sur les données ;
- concevoir une sécurité pour les données.

### Module 10 : Création d'une conception de sécurité pour la transmission des données

*Ce module décrit les menaces et les risques pesant sur la transmission des données. À la fin de ce module vous serez à même de concevoir la sécurité pour la transmission des données.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques pesant sur la transmission des données ;
- concevoir une sécurité pour la transmission des données.



## Cours :

# MS 2113 Conception de la sécurité pour les réseaux Microsoft (fin)

### Module 11 : Création d'une conception de sécurité pour les périmètres du réseau

*Ce module 11 décrit les menaces pesant sur les points auxquels votre réseau est connecté à d'autres réseaux, comme Internet. À la fin de ce module, vous serez à même de concevoir la sécurité pour les périmètres du réseau.*

#### Compétences acquises :

- déterminer les menaces et analyser les risques qui pèsent sur les périmètres d'un réseau ;
- concevoir une sécurité pour les périmètres des réseaux.

### Module 12 : Conception de réponses aux incidents de sécurité

*Ce module 12 fournit des informations sur l'audit et la création de procédures destinées à vous aider dans la conception de réponses aux incidents de sécurité. À la fin de ces travaux pratiques, vous serez à même de concevoir une stratégie d'audit et des procédures de réponse aux incidents.*

#### Compétences acquises :

- expliquer l'importance de l'audit et de la réponse aux incidents ;
- concevoir une stratégie d'audit ;
- concevoir une procédure de réponse aux incidents.

## Annexes

### Annexe A : Conception d'une stratégie du bon usage

*Cette annexe fournit des informations sur la création de stratégies destinées à vérifier que les utilisateurs utilisent les ressources réseau de manière acceptable.*

### Annexe B : Conception de stratégies pour la gestion des réseaux

*Cette annexe contient des instructions permettant d'assurer une gestion sécurisée du réseau par les administrateurs.*

### Annexe C : Conception d'une structure opérationnelle pour la gestion de la sécurité

*Cette annexe explique comment créer une structure permettant d'assurer la sécurité d'un réseau lorsque des modifications y sont apportées et à mesure que les besoins de l'organisation en matière de sécurité évoluent.*