

## Guide Microsoft pour la sécurité à l'intention des développeurs

### Infos Générales



**Public visé :** Les participants sont des développeurs professionnels, responsables de l'étude et du développement d'applications, de composants, de services de données centraux ou clients, écrits en Microsoft Visual Basic, en Microsoft Visual C++ ou en C#.



**Objectifs :** À la fin de ce séminaire, les participants seront à même d'effectuer les tâches suivantes : comprendre les raisons de l'informatique de confiance ; identifier les applications potentiellement hostiles ; identifier les principaux types d'attaques ; comprendre les conséquences d'une sécurité faible ; reconnaître des exemples d'intrusions ; identifier les défis auxquels vous devez faire face en mettant en oeuvre la sécurité ; comprendre la nécessité d'améliorer le processus tout au long du développement ; décrire le cadre de la sécurité ; comprendre la chronologie du développement d'un produit sécurisé ; décrire les principes d'une conception qui prend en compte la sécurité ; comprendre l'importance de la sécurité des données ; identifier les scénarios des menaces ; cibler contre qui nous devons nous défendre ; décrire les attaques les plus courantes ; décrire les fonctionnalités de sécurité de Microsoft .NET Framework ; expliquer comment fonctionne la sécurité de l'accès au code ; expliquer comment fonctionne la sécurité fondée sur des rôles ; expliquer comment utiliser la cryptographie pour signer et vérifier des données ; améliorer la sécurité pour les applications Web ASP.NET ; améliorer la sécurité pour les services Web ASP.NET ; appliquer les conseils pour écrire du code sécurisé avec .NET Framework.



**Pré requis :** Pour suivre ce séminaire, les stagiaires doivent : posséder une expérience du développement avec Microsoft Visual Basic, Microsoft Visual C++ ou C# ; avoir construit des applications Windows ou Web avec .NET Framework.

### infos pratiques

#### Référence

MS2806

#### Vos contacts

Christelle et Caroline

#### Certification

Pas de certification

#### Formateur

MCSE

#### Support

Microsoft Officiel

#### Durée



#### Repas



#### Café



#### Module 1 : Les bases de la sécurité d'une application

Ce module présente les connaissances élémentaires pour la création d'applications particulièrement sûres. Il couvre des concepts importants pour la sécurité et montre l'importance de prendre en compte la sécurité à chaque étape du développement. En outre, il décrit comment utiliser diverses technologies pour accroître la sécurité des communications et des données.

#### Module 2 : Meilleures pratiques pour écrire un code plus sûr

Ce module décrit les meilleures pratiques pour appliquer les principes de sécurité tout au long du processus de développement. Cette session décrit aussi les outils et les méthodologies de modélisation des menaces, et leur application pour réduire les vulnérabilités et limiter les risques d'une attaque.

#### Module 3 : Protection envers les menaces

Ce module se base sur la connaissance actuelle des meilleures pratiques de sécurité et sur la modélisation des menaces pour identifier une gamme de scénarios de menaces. Il décrit des stratégies efficaces pour se protéger contre des menaces très répandues, comme des dépassements de tampons mémoire, des scripts inter-sites, l'injection SQL et des attaques par déni de service.

#### Module 4 : Implémentation de la sécurité dans une application en utilisant .NET Framework

Ce module décrit comment implémenter des fonctions de sécurité additionnelles pour des applications qui sont construites sur .NET Framework. Il montre comment utiliser à la fois la sécurité de l'accès au code et la sécurité fondée sur les rôles pour limiter les vulnérabilités. Il explique comment exploiter la prise en charge de la cryptographie dans .NET Framework pour crypter et signer des données. Enfin, il montre comment sécuriser des applications Web et des services Web construits sur ASP.NET.