



Sécurité SOA



Descriptif

Traditionnellement, les fonctionnalités d'une application sont disponibles uniquement dans son contexte. Les autres applications ne peuvent aisément les réutiliser. SOA permet de surmonter cette difficulté en exposant les fonctionnalités de l'application comme «services ». Ces services peuvent être réutilisés par d'autres applications. Cependant ce processus n'est pas sans conséquence pour la sécurité des données. Dans ce module nous montrons pourquoi SOA rend inefficaces les approches traditionnelles de sécurisation des applications.

Cette formation permet aux participants de comprendre les nouvelles approches de sécurité rendues possible par SOA. Ces techniques permettent d'assurer la sécurité des données sans affaiblir les avantages liés à l'utilisation de la démarche SOA.

Durée :

1 jour

Objectifs :

- Acquérir les concepts, les méthodes et les outils pour une action de changement efficace au sein d'une conduite de projet
- Lier la décision stratégique à la mise en œuvre d'un projet : mesurer l'importance du facteur humain afin d'évaluer les pièges et les potentialités

PUBLIC

Décideurs
Chefs de projets
Experts métier
Analystes
Concepteurs
Développeurs

Introduction SOA

- Motivation pour adopter SOA
- Principes de base de SOA
- La notion de service

Aspects fonctionnels de la sécurité et SOA

- Authentification
- Autorisation
- Confidentialité
- Intégrité
- Protection contre les attaques

Aspects non fonctionnels de la sécurité et SOA

- Interopérabilité
- Manageabilité
- Simplicité de développement

Sécurité au niveau message (message-level security)

- WS-Security

Sécurité comme service (security as a service)

- Security Assertion Markup Language (SAML)
- WS-Trust

Sécurité dirigée par la politique (policy-driven security)

- WS-SecurityPolicy

Commandez votre session inter/intra au tél. 01 44 94 92 50

Prochaines sessions inter-entreprise :
6-7 juillet – 6-7 octobre – 21-22 décembre