# PLAN DE COURS

# SECURITE DES APPLICATIONS WEB

## Objectif

Découvrir tous les aspects de la sécurisation des architectures Web applicatives et notamment des solutions basées sur J2EE et .NET. Apprendre à mettre en oeuvre ces principes depuis le développement jusqu'au déploiement.

## Public Concerné

Chefs de projets, responsables sécurité, développeurs.

## Pré-requis

Connaissances de bases du développement d'applications Web et des outils de développement associés.

## Code

SEB100-3

## Durée

3 jours

## Programme

- RAPPELS SUR LES ARCHITECTURES WEB
  - Le serveur Web et le protocole http
  - Le serveur Apache
  - Le serveur IIS
  - Les serveurs applicatifs J2EE
  - Les serveurs applicatifs .NET
- LES PRINCIPES DE BASE DE LA SECURITE
  - Les objectifs
    - authentification
    - non répudiation
    - intégrité
    - confidentialité
    - traçabilité
  - Les types de risques
    - Risques liés à l'ouverture du système d'information à Internet
    - Risques spécifiques des architectures multi-tiers
  - Démarche sécurité pour les projets
    - Analyse de la vulnérabilité
    - Définition des responsabilités
    - Méthodologie appliquée aux différentes phases d'un projet
    - Les normes et méthodes existantes
  - Les infrastructures à clés publiques
    - La cryptographie à clé secrète, le hachage
    - La sécurisation par clé publique, les signatures numériques
    - Les certificats X509
    - PKI et les certificats, les autorités et opérateurs de certification
    - Les différentes offres et standards de PKI
    - Les standards spécifiques aux Web services (XKMS, SAML, XACML etc.)
- SECURITE DES ARCHITECTURE WEB
  - Architecture des applications Web
    - Les éléments constitutifs d'une architecture Web
    - Les vulnérabilités associées
  - Les systèmes de sécurisation
    - Les protocoles HTTPS et SSL
    - Les VPN et IPSec
    - Le courrier sécurisé S/MIME
    - L'authentification par un annuaire LDAP
    - Authentification centralisée (Kerberos, SSO, OTP)
    - L'authentification par biométrie
    - La sécurité de Windows et de Linux
    - Les solutions de pare feu
    - Les Proxy
  - Sécurité en environnement J2EE
    - Mécanismes de sécurité de J2EE 1.4
    - La JVM et SandBox
    - Le service JAAS d'authentification
    - L'extension JCE de cryptographie
    - La classe KeyStore pour stocker les clés et certificats
    - L'implémentation de SSL dans JSSE
    - Exemple de la bibliothèque open source Bouncy Castle
  - Sécurité en environnement .NET
    - Mécanismes de sécurité de .NET
    - Les stratégies de sécurité dans le CLR
    - Les couches d'authentification
    - La classe System.Security.Cryptography
    - L'interface CryptoAPI
    - La faille « Man in the Middle » dans CryptoAPI