

## Sécurité Java et JEE

Durée: 3 jours

Prix et dates: nous consulter

### Public:

Tout développeur souhaitant maîtriser la sécurité des applications Java et Jee.

### Objectifs:

Connaître les risques potentiels dans l'utilisation de Java, et les parades à mettre en oeuvre, les moyens de sécuriser les applications JEE.

### Connaissances préalables nécessaires:

Il est demandé aux participants de connaître les notions de base du langage Java.

### Programme:

- Besoins** : Les risques  
Politique de Sécurité  
Evaluation des risques en fonction des différents modes d'utilisation de Java (applets, application, servlets)
- Sécurisation de la JVM** : Limites naturelles imposées par Java : gestion mémoire.  
Contrôle du bytecode par la machine virtuelle.  
Mise en oeuvre du SecurityClassLoader
- Protection de l'exécution** : Exécution protégée : SecurityManager, ClassLoader.  
Surcharge des méthodes d'accès : lecture, écriture, exécution, ouverture de socket, autorisation de connexions...  
TP : Protection des accès sur le disque local d'une application.
- Chiffrement** : Les mécanismes de signature. Création de clés publiques et privées.  
Les clés RSA, DSA.  
Signature d'un document.  
Les algorithmes SHA1withDSA, MD5withRSA.  
Les MessageDigest. Les algorithmes MD2, MD5, SHA-1, SHA-512  
TP : Vérification de l'authenticité d'un document

## Sécurité Java et JEE

- Certificats** : Cycle de vie d'un certificat. La fabrique de certificats Java.  
Les certificats de modification X509.
- Contrôle** : Rappel sur les ACL. Le paquetage java.security.acl. Ajout d'entrée, vérification d'accès.
- Obfuscation** : Principe  
Techniques d'obfuscation  
Solutions commerciales
- JAAS** : Présentation  
Fonctionnement et mise en oeuvre
- Sécurité Jee** : Exemples avec WebSphere et JBoss  
Le service de sécurité  
Sécurité Web et EJB  
Autorisations EJB V3  
Accès applicatifs et lien avec un annuaire Ldap  
Mise en oeuvre des certificats avec JEE.