

## Java/JEE, application security



SII-196    3 Days (21 Hours)

### Description

This training will allow you to understand the security management mechanisms offered by Java, thanks to the theoretical study of the concepts and their progressive implementation, within standalone applications, JEE application servers as well as SOAP and REST web services.

### Who is this training for ?

#### For whom

Developers and project managers required to secure Java and JEE applications.

#### Prerequisites

Aucune

### Training objectives

- Implement security at the Java virtual machine level Leverage specific APIs such as JAAS, JSSE and JCE to secure your applications
- Secure your web services with the WS-Security and OAuth APIs

### Training program

#### Présentation des concepts liés à la sécurité

- Identification and authentication methods.
- Authorizations and permissions.
- Confidentiality, non-repudiation, encryption, public/private keys, certificate authorities.
- Firewalls and DMZ, protocol breakage.
- Types of attacks.

#### Sécurité de la machine virtuelle Java

- Loading classes.
- Sandbox concept.
- SecurityManager, AccessController and definition of permissions (files. policy).
- Create your permissions with Java Security Permission.
- Mechanisms to protect bytecode integrity, decompilation and code obfuscation.
- Specificities of Applets in terms of security.
- Practical work Definition of .
- specific policies.

### Java Authentication and Authorization Service

- JAAS architecture.
- Authentication via PAM, notion of Subject and Principal.
- Permission management, files.
- policy.
- Use JAAS with Unix or Windows, JNDI, Kerberos and Keystore.
- SSO support.
- Practical work Configure the policy. access control, implementation of authentication.

### SSL avec Java

- Functions of Java Secure Socket Extension (JSSE).
- Authentication via X certificates.
- 509.
- TLS and SSL.
- Encryption based on public keys, Java Cryptography Extension (JCE).
- Using SSL with HTTP.
- Practical work Configure SSL and implementation of SSL sockets.
- Use JDK tools (Keystore).

### La sécurité d'une application JEE

- Web and EJB container-level authentication.
- Application roles, permissions and XML deployment descriptors.
- Dynamic controls via Servlets and EJB APIs.
- Security in APIs: JDBC, JNDI, JTA, JMS, JCA.
- Practical work Security of an application deployed in Tomcat.

### La sécurité des services web SOAP

- Security at HTTP level.
- Security at SOAP & WSDL level with WS-Security (WSS4J, XWSS.
- ) & WS-Policy.
- WS-Security SOAP handlers using JAAS.
- Practical work Practical use with an implementation of WS-Security (XWSS).

### La sécurité des services web REST

- Using SSL with JAX-RS.
- The contributions of OAuth (authentication on the Internet).
- OAuth 1.
- 0 and 2.
- 0.
- Practical work Practical work with an Apache CXF implementation of JAX-RS.