

Formation Manipuler les certificats SSL

Code : SEC-SSL-100

Durée : 2 jours (14 heures)

Public visé

RSSI, DSI, administrateurs système et réseau, techniciens de maintenance système et réseau, consultants en cybersécurité.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Déterminer et préconiser des pratiques et outils de chiffrement
- Reconnaître les éléments structurant une PKI
- Identifier les étapes nécessaires à son implémentation

Programme

Jour 1 - Matin : Les techniques de chiffrement

- La sécurité par le chiffrement
- Les services offerts par le chiffrement
- Les chiffrements symétriques
- Les chiffrements asymétriques
- La cryptanalyse
- Les attaques sur les méthodes de chiffrement
- Les principaux algorithmes et techniques (AES, RSA, ECC...)
- Les protocoles liés aux PKI (LDAP, SCEP, OCSP...)

Jour 1 - Après-midi : Introduction aux systèmes d'infrastructure à clés publiques

- Les rôles et objectifs des infrastructures de gestion des clés
- Le positionnement des PKI dans le système d'information
- La gestion des clés cryptographiques
- Les composants d'une PKI (Autorité de Certification, Autorité d'Enregistrement)
- Les types d'architectures de gestion des clés
- Les bonnes pratiques et recommandations de mise en oeuvre

- Le cycle de vie (Demande, Génération, Affectation, Renouvellement, Révocation/Répudiation)
- Les certificats de type X.509
- Les certificats d'autorité
- Les listes de révocation
- L'audit et la conformité dans une PKI

Travaux pratiques : Mise en place d'une PKI avec Windows Server autonome ou sous Linux avec OpenSSL ou EJBCA

Jour 2 - Matin : PKI dans un environnement Microsoft Active Directory

- Gérer une PKI dans une infrastructure complexe
- Configurer un template de certificat
- Configurer "Certificate Enrollment"
- Archiver et récupérer un certificat
- Configuration entre deux organisations
- Deploying Smart Cards

Jour 2 - Après-midi : PKI dans un environnement Microsoft Active Directory - Suite

- Intégrer la PKI (Services SSL, Scripts Powershell, Technologies VPN, Technologies IPsec)

Travaux pratiques : Ajouter une PKI d'entreprise à la PKI autonome et à l'annuaire de l'entreprise ; Signer les scripts de l'organisation par la PKI

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}