PKI MISE EN œUVRE

Public	Ingénieurs, administrateurs systèmes et réseaux.
Durée	4 jours - 28 heures
Pré-requis	Bonnes connaissances en systèmes, réseaux et sécurité informatique.
Objectifs	Appréhender les différents algorithmes de chiffrement symétrique et asymétrique Mettre en oeuvre une hiérarchie d'autorités de certification Mettre en oeuvre une messagerie sécurisée Mettre en oeuvre une authentification forte par certificat X509
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Planning	Du 22/09/2025 au 25/09/2025 Du 15/12/2025 au 18/12/2025
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

INTRODUCTION

- Les faiblesses des solutions traditionnelles.
- Pourquoi la messagerie électronique n'est-elle pas sécurisée ?
- Peut-on faire confiance à une authentification basée sur un mot de passe ?
- Usurpation d'identité de l'expéditeur d'un message.

CRYPTOGRAPHIE

- Concepts et vocabulaire.
- Algorithmes de chiffrement symétrique et asymétrique.
- Fonctions de hachage : principe et utilité.
- Les techniques d'échange de clés.
- Installation et configuration d'un serveur SSH.
- SSH et Man in the Middle.
- SSH, l'usage du chiffrement asymétrique sans certificat.

CERTIFICATION NUMÉRIQUE

- Présentation du standard X509 et X509v3.
- Autorités de certification.
- La délégation de confiance.
- Signature électronique et authentification.
- Certificats personnels et clés privées.
- Exportation et importation de certificats.

L'ARCHITECTURE PKI

- Comment construire une politique de certification ?
- Autorité de certification. Publication des certificats.
- Autorité d'enregistrement (RA).
- Modèles de confiance hiérarchique et distribuée.
- Présentation du protocole LDAP v3.
- Mise en oeuvre d'une autorité de certification racine.
- Génération de certificats utilisateurs et serveurs.

GESTION DES PROJETS PKI : PAR QUELLES APPLICATIONS COMMENCER ?

- Les différentes composantes d'un projet PKI.
- Choix des technologies.
- La législation.

PANORAMA DES OFFRES DU MARCHÉ

- L'approche Microsoft.
- Les offres commerciales dédiées : Betrusted (ex-Baltimore) et Entrust.
- OpenPKI : la communauté Open Source.
- IdealX, entre solution commerciale et Open Source.
- Les offres externalisées Certplus, Versign...

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 27/02/2024