GESTION DES IDENTITÉS ET SÉCURITÉ DES ACCÈS

Public	Ingénieurs système, ingénieurs en sécurité, administrateurs système, chefs de projets en sécurité, MOE (maîtres d'oeuvre) et/ou MOA (maîtres d'ouvrage).
Durée	4 jours - 28 heures
Pré-requis	Avoir des connaissances de base sur la sécurité des systèmes d'information et une bonne maîtrise des systèmes et des infrastructures.
Objectifs	Renforcer la sécurité et simplifier l'accès aux informations pour les organisations Etendre le Single Sign-On (SSO) Intégrer une Public Key Infrastructure (PKI) Evaluer les services Cloud sur l'authentification à l'intérieur d'un système d'information (SI) Mettre en oeuvre un système de fédération.
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
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.

1. ETAT DE L'ART DE L'IAM (IDENTITY AND ACCESS MANAGEMENT)

- Constat d'hétérogénéité du SI
- Centralisation de l'information
- Gestion à partir d'un point d'accès unique
- L'autorisation
- L'administration et la gouvernance des identités
- Les bases de données d'authentification
- L'annuaire centralisé vs l'approche fédérative
- Les protocoles d'authentification
- Les bases de données d'authentification

2. IMPLÉMENTATION D'UNE SYSTÉMIQUE CRYPTOGRAPHIQUE

- Le chiffrement : symétrique, asymétrique
- La signature numérique
- Notion de certificats
- Certificats X.509 v3 pour les PKI
- Contrôler l'accès avec les certificats d'attributs
- Elaborer une stratégie de gestion des certificats
- Sécurisation des clés privées
- Utiliser un agent de récupération des clés
- Associer des identités à des certificats
- Publier les listes des certificats révoqués
- Evaluer les relations de confiance avec les CA (Certificate Authorities) externes

3. FÉDÉRER DES IDENTITÉS AVEC MICROSOFT ADFS 3.0 ET AZURE

- Authentification locale, accès distant
- Garantir l'interopérabilité et la portabilité des identités
- Concevoir des applications basées sur les revendications avec SAML
- Abstraction des protocoles WS-Trust et WS-Federation
- Partage des identités avec le Cloud
- Développer l'AD (Active Directory) sur site pour l'hébergement Azure
- Mettre en oeuvre l'authentification unique avec Azure pour les applications SaaS
- Fédération Amazon AWS
- S'authentifier avec les rôles IAM d'Amazon
- Connexion Microsoft fédérée aux services et aux instances Amazon

4. GESTION DES IDENTITÉS POUR LES APPAREILS MOBILES

- Les problèmes nouveaux : les smartphones et tablettes, le mode déconnecté pour les mobiles avec bases de données intégrées
- La mode du BYOD (Bring Your Own Device) et ses conséquences
- La restriction des périmètres fonctionnels
- La mode du BYOID (Bring Your Own IDentity) : "Apportez votre identité"
- Contrôle des coûts d'implémentation
- Réduit le coût total de possession
- Zero Trust : la solution idéale pour réduire l'exposition
- Configurer le protocole d'inscription des certificats simples
- AWS, Azure, Microsoft et les solutions pour le BYOD

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

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

E-mail
contact@audit-conseil-formation.com

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

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation