BIG DATA, SÉCURITÉ DES DONNÉES

Public	Consultants sécurité et SI, administrateurs système.
Durée	2 jours - 14 heures
Pré-requis	Notions d'architectures applicatives. Avoir de bonnes connaissances dans la sécurité réseau et système, connaitre les plateformes Hadoop.
Objectifs	Comprendre la qualification complexe des données Identifier les principaux risques touchant les solutions de traitement des données massives Maîtriser le cadre juridique (CNIL et PLA (Privacy Level Agreement)) Connaître les principales solutions techniques de base pour se protéger des risques Mettre en oeuvre une politique de sécurité pour traiter les risques, les menaces, les attaques
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. RISQUES ET MENACES

- Introduction à la sécurité. Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).
- Etat des lieux de la sécurité informatique.
- Le vocabulaire de la sécurité informatique.
- La classification DICT/P : Disponibilité, Intégrité, Confidentialité et Traçabilité/Preuve.
- Attaques "couches basses". La sécurité sur Hadoop. Intelligence gathering.
- Forces et faiblesses du protocole TCP/IP. HTTP : protocole exposé (SQL injection,Cross Site Scripting, etc.).
- Illustration des attaques de type ARP et IP Spoofing, TCPSYNflood, SMURF, etc
- Déni de service et déni de service distribué. DNS : attaque Dan Kaminsky. Attaques applicatives.

2. ARCHITECTURES DE SÉCURITÉ

- Quelles architectures pour quels besoins ?
- Plan d'adressage sécurisé : RFC 1918. Translation d'adresses (FTP comme exemple).
- Le rôle des zones démilitarisées (DMZ). Exemples d'architectures.
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité, firewalls et environnements virtuels.
- Proxy serveur et relais applicatif. Proxy ou firewall : concurrence ou complémentarité ?
- Evolution technologique des firewalls (Appliance, VPN, IPS,UTM...).
- Reverse proxy, filtrage de contenu, cache et authentification. Relais SMTP : une obligation ?

3. VÉRIFIER L'INTÉGRITÉ D'UN SYSTÈME

- Les principes de fonctionnement.
- Quels sont les produits disponibles ?
- Présentation de Tripwire ou AIDE (Advanced Intrusion Detection Environment).
- L'audit de vulnérabilités.
- Principes et méthodes et organismes de gestion des vulnérabilités.
- Site de référence et panorama des outils d'audit.
- Définition d'une politique de sécurité.
- Etude et mise en œuvre de Nessus (état, fonctionnement, évolution).

4. LES ATTEINTES JURIDIQUES AU SYSTÈME DE TRAITEMENT AUTOMATIQUE DES DONNÉES

- Rappel, définition du Système de Traitement Automatique des Données (STAD).
- Les risques sur les solutions de traitement des données massives.
- Types d'atteintes, contexte européen, la loi LCEN. Le règlement RGPD, CNIL, PLA.
- Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

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