SÉCURITÉ DU SI LES FONDAMENTAUX

Public	Responsables de l'informatique Administrateurs réseaux Techniciens Webmasters Responsables de la sécurité informatique
Durée	4 jours - 28 heures
Pré-requis	Il est nécessaire d'avoir une bonne connaissance générale des réseaux et des systèmes d'exploitation courants
Objectifs	Pouvoir évaluer les risques internes et externes liés à l'utilisation d'Internet Comprendre quels sont les mécanismes qui permettent de garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes Disposer d'une première approche des concepts techniques, pour comprendre la sécurité des systèmes d'information
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. L'ENVIRONNEMENT

- Le périmètre (réseaux, systèmes d'exploitation, applications)
- Les acteurs (hackers, responsables sécurité, auditeurs, vendeurs et éditeurs)
- La veille technologique
- Les organismes officiels

2. LES MÉTHODES DES ATTAQUANTS

- Les scénarios d'attaques intrusion, DDOS, ...
- Les attaques sur les protocoles réseaux
- Les faiblesses des services :Web, VoIP, Messagerie
- Le code vandale : virus, vers et chevaux de Troie

3. LA SÉCURITÉ DES ACCÈS, FIREWALL, WAF, PROXY,NAC

- L'accès des stations aux réseaux d'entreprise,802.1X, NAC
- Les différents types de firewalls
- Les règles de filtrage
- Les règles de la translation d'adresse (NAT)
- La mise en oeuvre d'une zone démilitarisée (DMZ)
- La détection et surveillance avec les iDS
- L'intégration d'un firewall dans le réseau d'entreprise
- La gestion et l'analyse des fichiers log

4. LA SÉCURITÉ DES SYSTÈMES D'EXPLOITATION

- Le Hardening de Windows
- Le Hardening d'Unix/Linux
- Le Hardening des nomades : IOS / Android

5. LA SÉCURITÉ DES APPLICATIONS AVEC EXEMPLE D'ARCHITECTURES

- Les serveurs et clients Web
- La messagerie électronique
- La VoIP IPbx et téléphones

6. LA SÉCURITÉ DES ÉCHANGES, LA CRYPTOGRAPHIE

- L'objectif du cryptage et fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap,chap,Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN réseau privé virtuel site à site et nomade

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