

Public	Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.
Durée	4 jours - 28 heures
Pré-requis	Bonnes connaissances en réseaux et systèmes.
Objectifs	<p>Connaître les failles et les menaces des systèmes d'information</p> <p>Maîtriser le rôle des divers équipements de sécurité</p> <p>Concevoir et réaliser une architecture de sécurité adaptée</p> <p>Mettre en oeuvre les principaux moyens de sécurisation des réseaux</p> <p>Sécuriser un système Windows et Linux</p>
Méthodes pédagogiques	<p>Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.</p> <p>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.</p> <p>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.</p>
Moyens techniques	<p>1 poste de travail complet par personne</p> <p>De nombreux exercices d'application</p> <p>Mise en place d'ateliers pratiques</p> <p>Remise d'un support de cours</p> <p>Passage de certification(s) dans le cadre du CPF</p> <p>Remise d'une attestation de stage</p>
Modalité d'évaluation des acquis	<p>Evaluation des besoins et objectifs en pré et post formation</p> <p>Evaluation technique des connaissances en pré et post formation</p> <p>Evaluation générale du stage</p>
Planning	<p>Du 10/09/2024 au 13/09/2024</p> <p>Du 03/12/2024 au 06/12/2024</p> <p>Du 10/02/2025 au 13/02/2025</p> <p>Du 22/09/2025 au 25/09/2025</p>
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.
- Etat des lieux de la sécurité informatique.
- Le vocabulaire de la sécurité informatique.
- Attaques "couches basses".
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, SMURF, etc.
- Déni de service et déni de service distribué.
- Attaques applicatives.
- Intelligence gathering.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- DNS : attaque Dan Kaminsky.

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.
- Actions et limites des firewalls réseaux traditionnels.
- Evolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
- Les firewalls et les environnements virtuels.
- Proxy serveur et relais applicatif.
- Proxy ou firewall : concurrence ou complémentarité ?
- Reverse proxy, filtrage de contenu, cache et authentification.
- Relais SMTP, une obligation ?

3. SÉCURITÉ DES DONNÉES

- Cryptographie.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services cryptographiques.
- Authentification de l'utilisateur.
- L'importance de l'authentification réciproque.
- Certificats X509. Signature électronique. Radius. LDAP.
- Vers, virus, trojans, malwares et keyloggers.
- Tendances actuelles. L'offre antivirus, complémentarité des éléments. EICAR, un "virus" à connaître.

4. SÉCURITÉ DES ÉCHANGES

- Sécurité WiFi.
- Risques inhérents aux réseaux sans fil.
- Les limites du WEP. Le protocole WPA et WPA2.
- Les types d'attaques.
- Attaque Man in the Middle avec le rogue AP.
- Le protocole IPSec.
- Présentation du protocole.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
- Les protocoles SSL/TLS.
- Présentation du protocole. Détails de la négociation.
- Analyse des principales vulnérabilités.
- Attaques sslstrip et sslsnif.
- Le protocole SSH. Présentation et fonctionnalités.
- Différences avec SSL.

5. SÉCURISER UN SYSTÈME, LE "HARDENING"

- Présentation.
- Insuffisance des installations par défaut.
- Critères d'évaluation (TCSEC, ITSEC et critères communs).
- Sécurisation de Windows.
- Gestion des comptes et des autorisations.
- Contrôle des services.
- Configuration réseau et audit.
- Sécurisation de Linux.
- Configuration du noyau.
- Système de fichiers.
- Gestion des services et du réseau.

6. AUDIT ET SÉCURITÉ AU QUOTIDIEN

- Les outils et techniques disponibles.
- Tests d'intrusion : outils et moyens.
- Détection des vulnérabilités (scanners, sondes IDS, etc.).
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.
- Réagir efficacement en toutes circonstances.
- Supervision et administration.
- Impacts organisationnels.
- Veille technologique.

7. ETUDE DE CAS

- Etude préalable.
- Analyse du besoin.
- Elaborer une architecture.
- Définir le plan d'action.
- Déploiement.
- Démarche pour installer les éléments.
- Mise en œuvre de la politique de filtrage.

NOUS CONTACTER

Siège social

16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone

04 76 23 20 50 - 06 81 73 19 35

Centre de formation

87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

E-mail

contact@audit-conseil-formation.com

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



ACF Audit Conseil Formation



@ACF_Formation



ACFauditconseilformation