CYBERSÉCURITÉ TESTER SES ENVIRONNEMENTS

Public	Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.
Durée	3 jours - 21 heures
Pré-requis	Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux).
Objectifs	Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques Mesurer le niveau de sécurité de votre Système d'Information Réaliser un test de pénétration
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 24/09/2025 Du 08/12/2025 au 10/12/2025
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.

LES ATTAQUES WEB

- OWASP : organisation, chapitres, Top10, manuels, outils.
- Découverte de l'infrastructure et des technologies associées, forces et faiblesses.
- Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.
- Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
- Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
- Evasion et contournement des protections : exemple des techniques de contournement de WAF.
- Outils Burp Suite, ZAP, Sqlmap, BeEF.

DÉTECTER LES INTRUSIONS

- Les principes de fonctionnement et méthodes de détection.
- Les acteurs du marché, panorama des systèmes et applications concernés.
- Les scanners réseaux (Nmap) et applicatifs (Web applications).
- Les IDS (Intrusion Detection System).
- Les avantages de ces technologies, leurs limites.
- Comment les placer dans l'architecture d'entreprise ?
- Panorama du marché, étude détaillé de SNORT.

LA COLLECTE DES INFORMATIONS

- L'hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, bases de données, etc.).
- La collecte passive en mode écoute et la collecte active.

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 : 12/12/2024