DEFENDRE LE PERIMETRE RESEAU CONTRE LES CYBERATTAQUES

Public	Les professionnels de la sécurité recherchant une connaissance et des capacités pour fortifier le périmètre de réseau et fournir une défense intégrée
Durée	4 jours - 28 heures
Pré-requis	Une connaissance pratique de TCP/IP et de l'architecture serveur client est utile.
Objectifs	Alors que les entreprises et les gouvernements continuent de se fier à Internet pour permettre les communications et l'accès aux données entre les employés, fournisseurs et autres partenaires, ils ont besoin de s'assurer de la confidentialité, de l'intégrité et de la disponibilité de ces informations. Dans cette optique, cette formation de niveau intermédiaire, apporte au personnel informatique et réseau les connaissances et les compétences dont ils besoin pour comprendre, mettre en oeuvre et gérer les éléments clés d'un réseau sécurisé.
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.

DÉFINIR DES PRINCIPES DE SÉCURITÉ

- S'assurer de la confidentialité, de l'intégrité et de la disponibilité des données (CIA)
- Évaluer les techniques de défense
- Définir une position de sécurité générique

DÉVELOPPER UNE STRATÉGIE DE SÉCURITÉ

- Équilibrer les risques et les exigences métier
- Identifier vos objectifs en assurance de l'information
- Choisir des technologies de sécurité

DÉPLOYER UN PARE-FEU SÉCURITÉ

- Déterminer le type de pare-feu adéquat
- Sélectionner/mettre en application le système d'exploitation
- Virtualiser un pare-feu

CONFIGURER LE PARE-FEU DE SORTE QU'IL PRENNE EN CHARGE LES SERVICES SORTANTS

- Prendre en charge des services simples : HTTP, SMTP
- Filtrer le contenu dangereux et gérer le trafic chiffré
- Gérer les services complexes : VoIP, audio et vidéo

FOURNIR DES SERVICES EXTERNES DE FAÇON SÉCURISÉE

- Mettre en œuvre des serveurs accessibles au public
- Créer une architecture de zone démilitarisée
- Prendre en charge le courrier SMTP

PERMETTRE L'ACCÈS AUX SERVICES INTERNES

- Personnaliser le DNS pour les architectures du pare-feu
- Configurer la translation d'adresse réseau
- Développer des listes d'accèspour les applications de serveurs clients

DÉTECTER ET PRÉVENIR LES INTRUSIONS

- Détections des anomalies et des mauvaises utilisations
- Analyse avancée

DÉPLOYER UN IDS

- Placer l'IDS du réseau (NIDS) au sein de l'architecture du réseau
- Exploiter des captures en mode discret

DÉTECTER LES INTRUSIONS DANS L'ENTREPRISE

- Concevoir une hiérarchie IDS multicouche
- Gérer l'IDS distribué
- Déployer un IDS hôte sur les serveurs critiques

INTERPRÉTER LES ALERTES

- Vérifier l'exploitation de l'IDS
- Minimiser les faux positifs et négatifs
- Valider les événements IDS et reconnaître les attaques

ARRÊTER LES INTRUS

- Exploiter les réponses actives de l'IDS
- Snipping une session TCP
- Contrôler l'accès avec une mise à jour du pare-feu
- Arrêter les paquets avec Gateway IDS (GIDS)

CRÉER DES TUNNELS VPN

- Tunnels obligatoires vs. tunnels volontaires
- Prendre en charge les utilisateurs à distance avec les tunnels au niveau de la couche 2, connecter des sites à distances avec des tunnels au niveau de la couche 3

APPLIQUER UNE PROTECTION CRYPTOGRAPHIQUE

- Vérifier l'intégrité du message avec le hachage
- S'assurer de la confidentialité avec le chiffrement symétrique
- Échanger les clés symétriques avec le chiffrement asymétrique
- Gérer les certificats numériques avec les PKI

CONFIGURER LES VPN DES UTILISATEURS À DISTANCE

- Déployer le logiciel client
- Exploiter le protocole de tunnellisation de niveau 2 (L2TP)
- Protéger les tunnels L2TP avec IPsec Transport Mode

CRÉER DES VPN SITE À SITE

- Utiliser des concentrateurs VPN et des routeurs VPN
- Appliquer IPsec en mode tunnel
- Évaluer les protocoles de tunneling

RÉDUIRE L'IMPACT DES ATTAQUES PAR DÉNI DE SERVICE (DOS)

- Minimiser les attaques à partir d'une connexion avec les IPS
- Blackholing et sinkholing
- Mettre en œuvre un système de défense par déni de service (DoS)
- Blacklister les sites et les plages d'adresse susceptibles d'attaquer

ARCHITECTURES DU PÉRIMÈTRE

- Intégrer l'IDS et les VPN dans l'architecture de votre pare-feu
- Positionner des serveurs accessibles en externe
- Surveiller et contrôler des réseaux sans fil

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 : 03/04/2020