SECURITE DES POINTS D'ACCES ET CONTROLEUR D'ACCES AU RESEAU

Public	Les professionnels de la sécurité recherchant à renforcer leur politique de sécurité pour la protection des données sensibles et traiter les menaces internes et externes
Durée	4 jours - 28 heures
Pré-requis	Les participants doivent avoir des connaissances de base sur TCP/IP, les commutateurs et l'Active Directory.
Objectifs	Les meilleures défenses de périmètre font peu pour contrecarrer les actions des utilisateurs relatives aux manigances de l'ingénierie sociale, la sélection d'un mot de passe faible et l'utilisation frauduleuse des réseaux sociaux. Cela place le fardeau de la sécurité dans un environnement de sécurité interne solide qui consiste en un contrôle de l'accès réseau et une sécurité bout à bout. De plus, les organisations ont besoin d'une dernière ligne de défense contre les pirates informatiques qui peuvent se frayer un chemin vers le périmètre.
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. DÉFENSES INTERNES VS. DÉFENSES DU PÉRIMÈTRE

- Définir une stratégie de sécurité globale
- Estimer les menaces intérieures et les attaques côté client
- Changer de paradigme

2. ÉTABLIR UNE ARCHITECTURE INTERNE SÉCURISÉE

- Établir une stratégie de contrôle d'accès basée sur le risque
- Choisir des stratégies d'accès sans fil et à distance
- Surveiller et contrôler le trafic réseau

3. DÉVELOPPER UNE STRATÉGIE VLAN

- Décider du nombre et du type de VLAN, configurer le trunking des VLAN et gérer les VLAN au niveau central

4. ISOLER LE TRAFIC

- Restreindre l'accès l'accès avec la sécurité des ports
- Définir les VLAN « quarantaine » et « invité «
- Activer les VLAN de gestion Out-of-Band (OOB)

5. INSTALLER UN SERVEUR NAC

- Déterminer le type de serveur NAC adéquat
- Exploiter l'infrastructure des VLAN

6. SÉCURISER L'ACCÈS AVEC 802.1X

- Installer les authentificateurs, authentifier avec les certificats et les serveurs RADIUS, refuser les appareils sauvages

7. EXPLOITER LE NAC POUR METTRE EN œUVRE DES SERVEURS DE STRATÉGIE

- Configurer les stratégies sur le serveur
- Mettre en application des BYOD avec la stratégie

8. GÉRER LES PATCHS ET DES MISES À JOUR ANTI-MALWARE

- Établir les espaces de stockage des logiciels
- Pousser les patchs de l'OS et des applidations vers les clients

9. SURVEILLER, JOURNALISER ET METTRE EN APPLICATION

- Réaliser une vérification du système
- Valider des profils avant et après connection
- Mettre en quarantaine les appareils non conformes

10. ÉTABLIR UNE POLITIQUE DE CHIFFREMENT

- Gérer les appareils mobiles et les médias amovibles
- Intégrer les techniques de Data Loss Prevention (DLP)

11. METTRE EN œUVRE LE CHIFFREMENT

- Exploiter les KPI pour générer une clé de récupération d'entreprise et mettre en application le chiffrement du disque entier pour le point de terminaison

12. DÉVELOPPER UNE STRATÉGIE DE PERTE DE DONNÉES

- Autoriser le trafic nécessaire et refuser le trafic dangereux
- Mettre les applications approuvées sur liste blanche
- Réguler les appareils joints USB

13. SURVEILLER ET DÉTECTER LA FUITE DE DONNÉES

- Prévenir les tunnels cachés au sein du trafic DNS et HTTP
- Retrouver les clients infectés

14. DÉPLOYER LES ANTI-MALWARE

- Pousser le logiciel défensif vers le point de terminaison avec la Protection d'accès réseau
- Établir des serveurs de mise à jour des signatures anti-malware internes et gérer les utilisateurs mobiles et à distance

15. UTILISER LES HONEYPOTS POUR LA DÉTECTION DE MALWARE ET DE BOTNET

- Sélectionner des honeypot virtuels ou physiques
- Déterminer le placement VLAN, surveiller les honeypots

16. DÉPLOYER DES IDS/IPS BASÉS SUR L'HÔTE/LE RÉSEAU

- Personnaliser l'IDS/IPS pour réduire les faux positifs
- Décider des options de déploiement

17. MINIMISER LES ATTAQUES ET Y RÉPONDRE

- Prévenir les fuites d'informations d'identification personnelle
- Analyser les réponses manuelles vs. automatiques
- Élaborer des stratégies de confinement

18. REPORTING ET VÉRIFICATION DE CONFORMITÉ

- Générer des rapports pour les systèmes conformes et non conformes
- SOX
- EISMA
- PCI
- HIPAA

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