ARUBA NETWORK SECURITY LES FONDAMENTAUX

Public	Ingénieurs réseau / du service d'assistance.
Durée	4 jours - 28 heures
Pré-requis	Avoir une expérience dans le domaine de la mise en réseau dans des environnements câblés et sans fils.
Objectifs	Définir la terminologie de la sécurité Durcir les devices Sécuriser un WLAN (Wireless Local Area Network) Sécuriser un réseau local câblé (LAN) Sécuriser le WAN Classifier les terminaux Détecter les menaces Analyser les dépannages Classifier les terminaux Effectuer des recherches Forensics.
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 16/09/2025 au 19/09/2025 Du 17/11/2025 au 20/11/2025
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.

MENACES POUR LA SÉCURITÉ ET STRATÉGIE DE SÉCURITÉ D'ARUBA

- Aperçu des menaces
- Etapes de l'attaque
- Stratégie de sécurité d'Aruba

TECHNOLOGIES DE SÉCURITÉ

- Conformité réglementaire
- Authentification, autorisation, comptabilité (AAA)

COMMUNICATIONS SÉCURISÉES

- Cryptage symétrique et authentification par hachage
- Cryptage asymétrique et certificats numériques
- TLS

DURCIR LES COMMUTATEURS D'ARUBA

- Aperçu du durcissement
- Mettre en place une gestion hors bande
- Authentifier les gestionnaires en toute sécurité
- Assurer la sécurité physique et autres mesures de renforcement

DURCIR LES DISPOSITIFS SANS FIL ARUBAOS

- Blocage de l'accès administratif
- Services de verrouillage
- Utiliser CPSec

RENFORCER LA SÉCURITÉ DES RÉSEAUX LOCAUX

- Protections Spanning Tree
- Snooping DHCP et protection ARP
- Technologies de routage sécurisé

TECHNOLOGIES D'AUTHENTIFICATION DES RÉSEAUX

- Authentification des réseaux
- Sécurité WLAN - Cryptage + Authentification

RENFORCER LA SÉCURITÉ EDGE GRÂCE À UNE INFRASTRUCTURE ARUBA

- Appliquer WPA3-Enterprise
- Appliquer 802.1X sur le réseau câblé

METTRE EN PLACE UN SYSTÈME D'AUTHENTIFICATION ET DE CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES

- Politiques Aruba de pare-feu basées sur les rôles
- Segmentation dynamique

IDENTIFIER ET CLASSER LES TERMINAUX

- Introduction à la classification des terminaux
- DHCP Fingerprinting avec les devices ArubaOS Mobility
- Aruba ClearPass Policy Manager Device Profiler
- ClearPass Device Insight

SÉCURITÉ DE LA BRANCH

- Introduction aux solutions Aruba SD-Branch

METTRE EN OEUVRE LA DÉTECTION DES MENACES ET LES FORENSICS

- Comprendre les Forensics
- Analyser les évènements ArubaOS WIP

DÉPANNAGE ET SURVEILLANCE

- Introduction au dépannage des problèmes d'authentification
- Utilisation des outils ClearPass pour résoudre certains problèmes courants
- Packet Capture
- Monitoring

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 : 29/09/2023