Sécurité des architectures

Référence : **SECARCHI** Durée : **4 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Bonnes connaissances en informatique et connaissances de base en sécurité. • 2-Très bonnes connaissances en réseaux (VLAN, pare-feux, etc), par exemple une certification CCNA+CCNP de Cisco ou NSE4 de Forninet ou CCSA de Checkpoint ou CSNA de Stormshield ou équivalent.

PROFIL DES STAGIAIRES

• 1-Architectes réseaux. • 2-Administrateurs systèmes et réseaux. • 3-Consultants en sécurité. • 4-Auditeurs en sécurité. • 5-RSSI.

OBJECTIFS

• Connaître les problématiques liées à l'architecture des réseaux complexes. • Connaître les solutions associées. • Savoir auditer une architecture. • Développer un plan d'évolution sécurisée d'une architecture.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Introduction générale

- Logistique
- Tour de table
- Objectifs de la formation
- Non-objectifs de la formation
- Signalétique

Introduction de la formation

- Principes d'architecture : Exposition / connectivité / attractivité
- Vocabulaire : Segmentation ; Risque ; Persona
- Lien avec d'autres domaines : Administration ; Urbanisation ; Gestion des risques
- Dessine-moi un schéma d'architecture

Notions de réseaux

- Modèles théoriques
- Quiz introductif
- Couche 2 – Liaison : Domaine de collision / domaine de diffusion ; Composants de base et adressage ; Segmentation – LAN / VLAN / PVLAN ; Sécuriser le lien local
- Couche 3 – Réseau : Composants de base et adressage ; Segmentation
- Échanges d'informations
- Composants spécifiques : Diode / WDM / sonde

Flux

- Filtrage
- Modes de connexion
- Chiffrement
- Authentification

Architecture de base : risques, points d'attention, contraintes et solutions

- Notion de bulle et niveaux : tiers-{0,2}
- Séparation des environnements : Production vs. hors-production
- Authentification et autorisation
- Administration : Zones d'administration ; Spécificités de Windows et Active Directory ; Postes d'administration
- Composants d'infrastructure et de sécurité : Services d'infrastructure ; Cas pratiques : DNS / supervision / sauvegarde / accès Internet / VPN
- Applications, 2-tiers / 3-tiers
- Continuité : Redondance et haute disponibilité ; Dépendance circulaire

Architectures spécifiques

- Virtualisation de l'infrastructure
- Cloud
- Sous-traitants
- Architectures industrielles & SCADA
- Gestion technique des bâtiments
- Divers
- ToIP / Wi-Fi / Grid / virtualisation et infrastructures « agiles » / IoT