EduGroupe
Accompagner pour réussir

Parcours métier d'Intégrateur Sécurité

Référence : **SECINTEG** Durée : **7 jours (49 heures)** Certification : **Aucune**

Connaissances préalables

- 1-Avoir suivi le Parcours Introductif Cybersécurité ou posséder les connaissances et compétences équivalentes
- 2-Connaître le guide d'hygiène sécurité de l'ANSSI

Profil des stagiaires

- Administrateurs Systèmes et Réseaux
- Architectes infrastructure
- Chefs de projet infrastructure
- Consultants
- Ingénieurs
- Responsables informatiques

Objectifs

- Comprendre les méthodologies d'implémentation des composants de la sécurité des systèmes d'information : Firewall / applicatif, IPS/IDS, SIEM, IAM)
- Savoir implémenter les composants de la sécurité des systèmes d'information
- Être capable de concevoir une infrastructure sécurisée comprenant des aspects d'accès distant, Cloud, Wifi et nomadisme

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

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

Contenu du cours

1. Jour 1

- Firewall / Proxy : Concept d'un Firewall / Proxy - Les types de pare-feu / Proxy - Les principales fonctions d'un pare-feu - Architecture et déploiement - Autres fonctionnalités du Pare-feu (Authentification, Administration, Log)
- IPS/IDS : Les types d'IDS / IPS - Les définitions (Alerte, Signature, NIDS, HIDS etc...) - Networks Intrusion Detection Systems (NIDS)
- Les définitions (Alerte, Signature, NIDS, HIDS etc...)
- Networks Intrusion Detection Systems (NIDS) : Décodeur de packet - Préprocesseurs - Le moteur de détection
- Host-Base Intrusion Detection Systems (HIDS) : Présentation du HIDS type OSSEC et architecture - Les signatures - Intégrité du système de fichier
- Quizz, Travaux pratiques sur l'implémentation d'un Firewall, NIDS et HIDS

2. Jour 2

- Scan de vulnérabilités : Présentation des produits - Composants et architectures de Nessus - Composants et architectures d'OPenVAs - Création de politique de Scan - Audit de configuration et de vulnérabilités - Analyse de rapport
- SIEM : Objectifs d'un SIEM - Architecture et fonctionnalités - Les timestamps (NTP) - Syslog et centralisation des journaux - Corrélation des événements
- Quizz, Travaux pratiques sur l'implémentation d'un scanneur de vulnérabilités
- Compréhension des logs et implémentation d'un SIEM

3. Jour 3

- VPN
- VPN les fondamentaux : VPN les fondamentaux - Tun - Tap
- Présentation et implémentation VPN IPSEC
- Présentation et implémentation VPN SSL / TLS
- Cas particulier du SSH
- Quizz, Travaux pratiques sur les différents types de tunnel/VPN

4. Jour 4

- 802.11 : 802.11 - Principes et caractéristiques - Attaques sur la technologie WiFi - Généralités - Le chiffrement - 802.1X - Mise en place d'une architecture WiFi sécurisée
- Mobilité :
- Les terminaux : Présentation et spécificités des mobiles, tablettes - Navigateurs, application client (user-agent) et son sandbox - Cloisonnement des fonctionnalités
- Le BYOD : Problématiques du BYOD, CYOD, COPE, BYOA - Enjeux du BYOD (sécurité, productivité, financier,...) -
- Premiers retours d'expérience : Problématique de nos données privées professionnelles - Solutions de virtualisation (vmWare, Citrix, Client Hyper-V), Desktops as a Service - Mobile Device Management : Présentation des solutions du marché (AirWatch, MobileIron, ...). Apple Configuration iPhone
- Quizz, Travaux pratiques sur l'implémentation d'une infrastructure wifi sécurisée ainsi que les terminaux.
- Travail personnel sur les notions abordées

5. Jour 5

- La sécurité du système et des équipements - Hardening Windows
- Gestion des accès et droits
- AV
- Cloisonnement
- Les mises à jours
- La sécurité des services et applications : EMET
- Défense en profondeur
- Intégrité du système
- Quizz, Travaux pratiques sur la sécurisation de poste Microsoft
- Travail personnel sur les notions abordées

6. Jour 6

- Hardening Linux :
- Gestion des accès et droits
- Sécurisation du kernel
- Cloisonnement
- Sécurisation des services
- Défense en profondeur
- Intégrité du système
- Quizz, Travaux pratiques sur la sécurisation de poste Linux
- Travail personnel sur les notions abordées

7. Jour 7

- Hardening Réseaux :
- Coupage en zone de sécurité
- Sécurité niveau 2
- Sécurité niveau 3
- Les produits et constructeurs d'équipement/outil de sécurité
- La veille
- Quiz, Travaux pratiques sur l'implémentation d'équipement réseau et de leurs sécurités
- Travail personnel sur les notions abordées (facultatif)

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.