Installer et administrer des solutions de sécurité

Hard Skills : Bureautique - Informatique -Comptabilité - Gestion

Informatique

Référence : 4-IT-IASS
Durée : 19 jours
Présentiel ou en classe à distance

Tarif Inter : 800 € Prix HT jour / personne
Tarif Intra : 1450 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2025 au 31/12/2025

Objectifs

Installation et administration de solutions sécurité

Prérequis

Pas de prérequis spécifiques

Public concerné

Toute personne en charge de cybersécurité

Contenu pédagogique

Introduction aux Critères Communs

- Projet Critères Communs, ses origines à son organisation actuelle
- Acteurs clés et sa déclinaison dans le schéma français géré par l'ANSSI
- Historique des principes de certification, du projet CC, des normes et des accords internationaux
- Philosophie de l'évaluation d'un produit et la terminologie CC
- Organisation du schéma français et les concepts de cible de sécurité

Remise à niveau Linux

- Système de fichiers
- Commandes de base
- Gestion des fichiers et répertoires
- Permissions Unix
- Gestion des entrées/sorties
- Gestion des tâches
- Edition de texte VI/VIM
- Archivage et la compression
- Authentification et comptes utilisateurs
- Shell
- Création et l'application de patch sur du code source
- Installation de packages
- Modules de sécurité
- Sécurisation des services
- Journalisation
- Pare-feu local

Conception, implémentation et sécurisation d'une infrastructure Windows Server

- Planifier et mettre en œuvre une infrastructure de déploiement serveur
- Planifier et mettre en œuvre les services de fichiers et de stockage
- Concevoir et mettre en œuvre une solution DHCP
- Concevoir et gérer une solution de gestion des adresses IP
- Mettre en œuvre une solution d'accès distant
- Concevoir et mettre en œuvre une solution de protection réseau
- Concevoir et mettre en œuvre une infrastructure de forêt et de domaine

- Concevoir une politique de stratégie de groupe
- Concevoir une stratégie de contrôleur de domaine
- Concevoir et mettre en œuvre une infrastructure pour une succursale
- Powershell
- Recommandations de sécurité
- Scénarios d'attaque classiques

Sécurité des systèmes et des réseaux

- Fondamentaux
- Architectures réseaux(rappels sur les réseaux IP, Couches OSI, Adressage, ARP, DNS, principales faiblesses de la pile TCP/IP, sécurisation des réseaux, les routeurs, virtualisation, équipements réseau, segmentation, filtrage, architecture (ANSSI)
- Périmètre (réseaux, systèmes d'exploitation, applications)
- Acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
- Risques, la protection, la prévention, la détection et la réaction

Durcissement Windows

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles
- Définir une politique de mises à jour sur les produits Microsoft
- Surveiller les mises à jour de sécurité des produits non-Microsoft
- Restreindre l'accès distant au parc Windows
- Mise en place d'alertes de sécurité sur le parc Windows
- Utilisation du pare-feu et d'un antivirus sur Windows
- Restreindre l'exécution des applications
- Utiliser les politiques de groupes (GPO)
- Auditer les politiques de groupes (GPO) avec Microsoft Security Compliance Manager
- Protection physique (clés USB, BIOS…)

Durcissement Linux

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles
- Définir une politique de mises à jour du noyau Linux
- Définir une politique de mises à jour des applicatifs tiers sur Linux
- Restreindre l'accès distant au parc Linux
- Mise en place d'alertes de sécurité sur le parc Linux avec un HIDS
- Utilisation du pare-feu et d'un antivirus Linux
- Restreindre l'exécution des applications et des commandes sur Linux
- Auditer les configurations

Mise en œuvre VPN

- Fondamentaux
- Mise en œuvre des différents types de VPN

Cryptographie

- Historique
- Introduction et enjeux de la cryptographie asymétrique
- Introduction au RSA, usage pour la distribution de clé et la signature
- Introduction à l'échange de clé Diffie-Hellman et aux courbes elliptiques.
- Génération des paramètres : nombres premiers, factorisation, etc.
- Cryptographie post-quantique
- Introduction et enjeux de la cryptographie symétrique
- Notions de chiffrement par blocs et chiffrement par flux

Mise en œuvre PKI

- Introduction
- Systèmes cryptographiques
- Infrastructure de gestion de clés
- Règles et recommandations générales

Virologie

- Introduction aux malwares (historique et évolution)
- Vecteurs d'infection
- Outils pour analyser les malwares

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants sous forme de réunion – discussion.
- Utilisation de cas concrets issus de l'expérience professionnelle.
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- Feuille de présence signée en demi-journée.
- Evaluation des acquis tout au long de la formation.
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2025

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2025

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55