

Sécurité systèmes et réseaux – Mise en oeuvre

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Systèmes et Réseaux

Action collective : Non

Filière : UNIX - CISCO

Rubrique : Les fondamentaux

Code de formation : S-RES

€ Tarifs

Prix public : 2995 €

Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

- **Le plan de développement des compétences** de votre entreprise : rapprochez-vous de votre service RH.
- **Le dispositif FNE-Formation.**
- **L'OPCO** (opérateurs de compétences) de votre entreprise.
- **Pôle Emploi** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
- **CPF -MonCompteFormation**

Contactez nous pour plus d'information

PRÉSENTATION

Objectifs & compétences

Savoir concevoir et réaliser une architecture de sécurité adaptée Mettre en oeuvre les principaux moyens de sécurisation des réseaux Disposer d'une première approche sur la sécurisation des serveurs Découvrir les obligations légales inhérentes à la sécurité

Public visé

Toute personne en charge de la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en place de serveurs d'entreprises

Pré-requis

Utilisation courante de Windows et des équipements constitutifs d'un réseau

📍 Lieux & Horaires

Campus : Ensemble des sites

Durée : 35 heures

Délaï d'accès :

Jusqu'à 8 jours avant le début de la formation

Distanciel possible : Oui

PROGRAMME

1. L'ENVIRONNEMENT

Le périmètre (réseaux, systèmes d'exploitation, applications)

Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)

Les risques

La protection La prévention La détection

2. LES ATTAQUES

Les intrusions de niveau 2 : au niveau du commutateur d'accès ou du point d'accès sans-fil
Les intrusions de niveau 3 (IP) : IP spoofing, déni de service, scanSniffer, man-in-the-middle, les applications stratégiques (DHCP, DNS, SMTP), les applications à risques (HTTP)

Les attaques logiques : virus, ver, cheval de troie, spyware, phishing, le craquage de mot de passe

Les attaques applicatives : sur le système d'exploitation ou sur les applications (buffer overflow)

3. LES PROTECTIONS

Au niveau des commutateurs d'accès : port sécurisé sur mac-adresse, utilisation du protocole 802.1x, VLAN Hopping, DHCP Snooping, IP source guard, ARP spoofing, filtre BPDU, root guard

Au niveau sans-fil : mise en place d'une clé WEP, de WPA, de WPA 2 (802.1i)

Au niveau IP : les pare-feux applicatifs, spécialisés, sur routeur, state full (inspection des couches au dessus de 3), les UTM, les proxys Protection des attaques logiques : les anti-virus, les anti spyware, le concept NAC

Protection des attaques applicatives : hardening des plates-formes Microsoft et Unix, validations des applicatifs

4. MONITORING ET PRÉVENTION

Sondes IDS SysLog

Serveur Exploitations des logs IPS : boîtiers dédiés, fonctionnalité du routeur

📅 Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

■ 23 / 09 / 2024

📍 : Ensemble des sites

✓ : Distanciel possible

🕒 : 35 heures

📅 : 5 jours

■ 07 / 10 / 2024

📍 : Ensemble des sites

✓ : Distanciel possible

🕒 : 35 heures

📅 : 5 jours

■ 18 / 11 / 2024

📍 : Ensemble des sites

✓ : Distanciel possible

🕒 : 35 heures

📅 : 5 jours

5. EXEMPLES D'ARCHITECTURES

Exemple d'une entreprise mono-site
Connexion des nomades
Exemple d'entreprise multi-site

6. LA SÉCURITÉ DES ÉCHANGES, LA CRYPTOGRAPHIE

L'objectif du cryptage et fonctions de base
Les algorithmes symétriques
Les algorithmes asymétriques
Les algorithmes de hashing Les méthodes d'authentification (pap,chap,Kerberos) Le HMAC et la signature électronique Les certificats et la PKI Les protocoles SSL IPSEC S/MIME Les VPN (réseau privé virtuel) de site à site et nomades

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise

Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom

Pendant la formation : mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels

Méthode

Fin de formation : entretien individuel

Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation

Assiduité : certificat de réalisation (validation des acquis)