DAWAN

Plan de la formation

www.dawan.fr

Formation Sécurité d'un accès à Internet

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	1 875,00 CHF HT (standard) 1 500,00 CHF HT (remisé)
Public :	Tous
Pré-requis :	Connaissances de Windows, Linux, Mac
Objectifs :	Comprendre les enjeux de la sécurité d'un accès Internet
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS444-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.

Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Introduction

Protocoles en jeu
Délimitation du périmètre à sécuriser
Définition des menaces, motivations

La menace externe

Parcours automatiques du réseau et scans
Déni de service
Intrusions
Perte d'information

Atelier pratique : détection et protection contre différents types d'attaque : SYN Flood, UDP flood, ICMP flood.

La menace interne

Vulnérabilité des postes clients
Sécurité et cloisonnement
Gestion des accès au réseau

Atelier pratique : surveillance d'un réseau interne, analyse des vulnérabilités d'un client

Protection

Réduction de la surface d'attaque
Définition du pare-feu
Filtrage entrant
Filtrage sortant

Atelier pratique : limitation des services sur un système linux, Windows

Mise en œuvre

Problématiques des attaques de masse et de l'exploitation du réseau
Limiter les risques d'intrusion sur Windows
Principes de configuration pour UNIX, Linux et Mac OS pour l'accès à Internet

Atelier pratique : mise en place d'un pare-feu, observations