DAWAN

Plan de la formation

www.dawan.fr

Formation Sécurité systèmes et réseaux – Mise en œuvre (Cybersécurité - Fondamentaux)

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 175,00 € HT (standard) 2 540,00 € HT (remisé)
Public :	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'entreprise (administrateurs systèmes / réseaux, intégrateurs, techniciens)
Pré-requis :	Bonnes connaissances générales des systèmes d'information, bases solides en réseaux TCP/IP et en administration de serveurs (Linux et/ou Windows).
Objectifs :	Savoir concevoir et réaliser une architecture de sécurité adaptée aux besoins de l'organisation - Mettre en œuvre les principaux moyens de sécurisation des réseaux (filtrage, segmentation, accès distants, protection périmétrique) - Disposer d'une première approche structurée de la sécurisation des serveurs (durcissement, mises à jour, droits, journaux) - Découvrir et comprendre l'apport de la cryptographie pour sécuriser les échanges d'informations
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 :	CYB445-F
Note de satisfaction des participants:	4,70 / 5
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 et enjeux de la cybersécurité

Panorama des menaces actuelles : ransomware, phishing, compromission de comptes, fuites de données
Principes de base : confidentialité, intégrité, disponibilité, traçabilité (CIA + logging)
Notions de conformité : RGPD, bonnes pratiques ANSSI, familles de normes ISO 2700x
Rôles et responsabilités : utilisateur, admin système/réseau, RSSI, prestataires
Atelier fil rouge : découverte du SI d’une PME fictive (cartographie rapide des actifs et premiers risques identifiés)

Analyse du risque et des menaces

Différencier menace, vulnérabilité, impact, probabilité, risque
Identifier les actifs critiques : données, services, utilisateurs sensibles, accès distants
Construire des scénarios de risques simples (ex. ransomware, compte VPN volé, poste admin compromis)
Introduire les bases d’une démarche d’analyse de risques (inspirée EBIOS / ISO 27005 sans formalisme lourd)

Atelier fil rouge : élaboration en groupe de 2 ou 3 scénarios de risques réalistes pour la PME fictive

Les différents niveaux de gestion de la sécurité

Sécurité organisationnelle : politiques, chartes, gestion des habilitations, sensibilisation utilisateurs
Sécurité des systèmes : postes de travail, serveurs, comptes d'administration, mises à jour
Sécurité réseau : segmentation, filtrage, accès distants, exposition Internet
Sécurité applicative : mises à jour, durcissement, gestion des accès, prise en compte OWASP au niveau macro
Atelier fil rouge : définition d'un plan de mesures de sécurité « par couches » pour le SI de la PME (données, systèmes, réseau, usage)

Sécurité des données

Identifier les données sensibles : données clients, RH, secrets techniques, sauvegardes
Contrôles d'accès : principes de moindre privilège, séparation des rôles, droits d'accès robustes
Sauvegardes et restauration : 3-2-1, tests de restauration, protection des sauvegardes contre le ransomware
Chiffrement des données au repos : disques, volumes, clés de chiffrement, bonnes pratiques
Atelier fil rouge : choix d'une stratégie de sauvegarde et de chiffrement adaptée aux données critiques de la PME

Sécurité des échanges de données

Contraintes de sécurité : intégrité, confidentialité, authentification, non-répudiation
Principes de chiffrement symétrique / asymétrique, certificats, PKI (niveau vulgarisation)
Sécurisation des échanges : HTTPS/TLS, VPN site à site et VPN nomade, email chiffré (vue d'ensemble)
Risques liés aux réseaux sans fil et aux accès distants (Wi-Fi invité, télétravail, BYOD)
Atelier fil rouge : définir les règles d'accès à distance (VPN, Wi-Fi, comptes) pour les collaborateurs de la PME

Sécurisation de Linux

Rappels sur les permissions standards et étendues (users, groups, sudo, ACL)
Durcissement de base d'un serveur Linux exposé (services, ports, mises à jour, SSH, journaux)
Introduction à PAM : principes, exemples simples (verrouillage de compte, contraintes de mot de passe)
Présentation des mécanismes de confinement (AppArmor, SELinux) et cas d'usage concrets
Pare-feu sur Linux (iptables/nftables) : règles simples de filtrage et journalisation basique
Surveillance et traces : journaux système (journald, syslog), introduction à auditd et fail2ban
Atelier fil rouge : durcir un serveur Linux de la PME (SSH, services, utilisateurs, pare-feu simple, première politique de logs)

Sécurisation de Windows (niveau fondamentaux)

Principes de sécurité Windows : comptes, groupes, UAC, mises à jour, antivirus / EDR
Bonnes pratiques sur un poste ou un serveur Windows membre d'un domaine (approche conceptuelle)
Gestion des droits et des partages : éviter les droits excessifs, comprendre les ACL de base
Pare-feu Windows et paramètres réseau : profils, règles entrantes / sortantes, diagnostics simples
Journal d'événements : savoir où chercher, types de journaux, premiers réflexes d'analyse
Atelier pratique : lecture de journaux Windows et identification de quelques événements de sécurité simples (logons, erreurs, services)

Sécurité réseau : mise en œuvre des protections et de la segmentation

Rappels : modèles de référence, IP, ports, services, exposition Internet
Segmentation réseau : VLAN, DMZ, zones utilisateurs / serveurs, accès administrateurs
Principes de filtrage : pare-feu, proxies, filtrage sortant, gestion des accès distants (VPN, bastions)
Introduction aux IDS/IPS et au monitoring réseau : concepts, positionnement dans l'architecture
Illustration avec un IDS open source (Suricata ou équivalent) via un exemple préparé (lecture d'alertes, types de détections) sans déploiement complet
Atelier fil rouge : proposer une architecture réseau segmentée et un schéma de filtrage pour la PME (Internet, Wi-Fi, VPN, serveurs internes)

Audit d’un système et amélioration continue

Objectifs d’un audit de sécurité : constat, priorisation, plan d’actions
Conduire un audit léger de configuration sur Linux et Windows : checklists et outils simples
Vérifier le cloisonnement applicatif et utilisateur, et les risques liés à la maintenance (versions, config, comptes techniques)
Introduire les bases de la supervision sécurité (SIEM / SOC) au niveau conceptuel : centralisation des logs, alertes, tableaux de bord
Atelier fil rouge : mini-audit final du SI de la PME (synthèse des mesures mises en place et priorisation des prochains chantiers)