DAWAN

Plan de la formation

www.dawan.fr

Formation Sécurité informatique : vocabulaire, concepts et technologies pour non-initiés

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	1 575,00 € HT (standard) 1 260,00 € HT (remisé)
Public :	Commerciaux, spécialistes du marketing, futurs consultants, chefs de projets ou responsables de formation amenés à évoluer dans l'univers de la sécurité informatique - Toute personne souhaitant comprendre la sécurité informatique pour optimiser sa collaboration avec les spécialistes du domaine
Pré-requis :	Maîtrise de base des usages numériques courants (messagerie, web, bureautique) ; aucun prérequis technique n'est nécessaire
Objectifs :	Comprendre les concepts, les technologies et les solutions de sécurité des réseaux informatiques pour pouvoir travailler avec les spécialistes et piloter les prestataires - Acquérir une vision globale et structurée de la sécurité informatique - Connaître les rôles des principaux intervenants du secteur et leurs métiers - Identifier les nouveaux enjeux associés à la sécurité informatique (cloud, télétravail, RGPD, IA, etc.)
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 :	CYB102740-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

Découvrir les fondamentaux et sécuriser les principaux domaines du SI

Comprendre ce que recouvrent les notions de sécurité informatique et de cybersécurité
Se familiariser avec les termes clés : menace, vulnérabilité, attaque, incident, risque, système d’information
Identifier les principaux domaines à sécuriser : postes de travail, serveurs, réseau, applications, cloud, mobilité
Relier les incidents de sécurité à des impacts très concrets pour l’entreprise (production, finances, image, juridique)
Atelier fil rouge : cartographier simplement le SI de son organisation et repérer les zones où la sécurité est la plus critique

Se protéger contre les malwares et les principales attaques

Identifier les grandes familles de menaces : virus, ransomwares, chevaux de Troie, phishing, attaques par mot de passe, fuites de données
Comprendre comment ces attaques se propagent : mails, pièces jointes,

téléchargements, sites piégés, supports amovibles
Découvrir les mesures de protection de base : mises à jour, antivirus/EDR, filtrage des mails, sauvegardes, bonnes pratiques utilisateurs
Voir le rôle des sensibilisations et des procédures dans la prévention des attaques
Atelier fil rouge : analyser 2 scénarios d'attaque (phishing et ransomware) et identifier les protections qui auraient pu limiter l'impact

Comprendre le fonctionnement des solutions de sécurité pour mieux protéger

Découvrir le rôle des pare-feux (firewalls) et du filtrage réseau
Comprendre à quoi servent les antivirus/EDR, les filtres web, les passerelles de messagerie sécurisées, les VPN
Introduire les notions de segmentation, DMZ, contrôle d'accès, authentification forte
Relier chaque solution à un ou plusieurs risques métiers (perte de données, interruption de service, vol de secrets, fraude)
Atelier fil rouge : associer des risques simples à des briques de sécurité (ex : « accès distant », « données sensibles », « site e-commerce »)

Exploiter les plates-formes spécialisées de sécurité et combiner les équipements

Comprendre ce que sont les plates-formes de sécurité : SOC, SIEM, consoles centralisées de supervision, outils de gestion de vulnérabilités
Voir comment les journaux (logs) et les alertes sont collectés, corrélés et suivis
Comprendre la notion de défense en profondeur : superposer plusieurs protections (poste, réseau, application, identité) plutôt que s'appuyer sur un seul outil
Identifier les limites d'une approche purement technique et l'importance de l'organisation et des procédures
Atelier fil rouge : construire un schéma « avant / après » en combinant plusieurs équipements pour sécuriser un SI type

Mesurer les impacts de la sécurité sur les usages, les métiers et la performance

Identifier les impacts possibles de la mise en place de la sécurité sur le quotidien des utilisateurs : contraintes, temps supplémentaire, nouvelles habitudes
Mesurer les impacts sur les systèmes : performance, disponibilité, maintenance, support
Comprendre les arbitrages à faire entre sécurité, confort, coût et agilité des métiers
Découvrir quelques indicateurs simples pour suivre la sécurité (incidents,

sensibilisations, mises à jour, résultats d’audits…)
Atelier fil rouge : lister les impacts positifs et négatifs d’une mesure de sécurité (ex : authentification forte) sur un service métier donné

S’appuyer sur les référentiels pour structurer la sécurité informatique

Découvrir les grands référentiels et bonnes pratiques : ISO 27001, guides de l’ANSSI, référentiels métiers, politiques internes
Comprendre la différence entre une norme, un guide de bonnes pratiques et une exigence réglementaire
Voir comment ces référentiels aident à structurer une démarche sécurité (gouvernance, procédures, contrôles)
Identifier ce que les non-techniciens peuvent en retenir pour dialoguer avec les spécialistes et les prestataires
Atelier fil rouge : repérer dans un exemple de référentiel quelques questions simples à poser à son prestataire ou à la DSI

Comprendre les grandes tendances de la sécurité informatique

Identifier les grandes évolutions : généralisation du cloud, télétravail, explosion des objets connectés, montée des ransomwares
Comprendre les nouveaux enjeux liés aux données (RGPD, protection de la vie privée, exigences clients et partenaires)
Aborder l’impact de l’IA sur la sécurité (attaques plus sophistiquées, automatisation de la défense, détection avancée)
Définir le rôle des non-spécialistes dans la sécurité future de l’organisation (alertes, remontée d’informations, participation aux projets)
Atelier fil rouge : définir 3 à 5 actions simples que peut engager un non-initié dans son poste pour contribuer à la sécurité