PROGRAMME DE FORMATION

Cybersécurité Entreprise SI

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0098	V2026-005	2 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
26 h	Distanciel asynchrone (e-learning) · Présentiel	11 modules 31 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

Inventorier et cartographier le système d'information d'une PME et prioriser sa sécurisation à l'aide d'un référentiel d'hygiène informatique.

Sécuriser les comptes et les accès : cycle de vie des comptes, authentification multifacteur, comptes d'administration séparés.

Organiser la gestion des mises à jour et des vulnérabilités, durcir et protéger les postes de travail.

Cloisonner et filtrer le réseau, sécuriser le Wi-Fi et les accès à distance, protéger la messagerie et les services en ligne.

Concevoir une politique de sauvegarde isolée et tester la restauration ; journaliser et repérer les signaux d'une compromission.

Préparer et conduire la réponse à un incident, encadrer les prestataires et piloter un plan de sécurisation conforme aux obligations applicables.

L'essentiel de la formation

Public visé

Responsables informatiques de TPE et PME, techniciens et administrateurs systèmes et réseaux, référents informatiques chargés de l'exploitation, prestataires d'infogérance de petites structures qui doivent sécuriser concrètement le système d'information d'une entreprise ; personnes en reconversion vers l'administration des systèmes qui en ont les bases.

Prérequis

Connaître les bases de l'administration informatique : comptes et droits sur un poste, installation d'un logiciel, notions de réseau (adresse IP, passerelle, DNS, Wi-Fi), messagerie professionnelle. Un positionnement en début de parcours le vérifie et déclenche une remise à niveau ciblée ; pour un public non technique, suivre plutôt WF-0262 « Cybersécurité -1 Panorama SSI ».

Aucune installation n'est exigée : les consoles d'administration sont reconstituées dans la plateforme ; un tableur et un traitement de texte servent à remplir les modèles fournis.

Modalités et déroulement

Formation à distance, accessible en ligne. Un positionnement court ouvre le parcours et déclenche, thème par thème, une remise à niveau ciblée si nécessaire. Un fil conducteur unique — la sécurisation du système d'information d'une PME de transport fictive — relie les dix modules : chaque geste est démontré, pratiqué en simulation guidée dans des consoles d'administration génériques reconstituées (signalées comme telles), puis refait en autonomie ou appliqué sur les modèles fournis (inventaires, matrices, politiques, plans). Chaque module se termine par une mise en situation qui livre une pièce du dossier de sécurisation. Aucune technique d'attaque n'est enseignée : les menaces sont étudiées par leurs effets et leurs traces. Temps de formation réparti à 60 % de pratique, 30 % de démonstrations et d'apports, 10 % d'évaluation. Les règles et délais ne sont jamais donnés de mémoire : chaque fiche mémo renvoie aux sources officielles relues à la date de production. Accompagnement par un formateur par messagerie.

Méthodes pédagogiques

- Positionnement en début de parcours
- Mises en situation et scénarios à décisions
- Production de livrables professionnels
- Quiz et QCM d'auto-évaluation
- Accompagnement et retours du formateur

Moyens pédagogiques et techniques

- Plateforme de formation en ligne, accès individuel à distance
- Modèles et supports téléchargeables
- Quiz et exercices interactifs en ligne
- Correction des productions sur grille de critères
- Messagerie avec le formateur

Modalités d'évaluation

Positionnement initial (non éliminatoire) ; vérification automatique de chaque simulation (gestes et état final de la configuration) ; correction des fichiers déposés critère par critère, avec corrigé ; livrable de fin de module vérifié sur grille critériée ; quiz de module ; évaluation finale composée d'un projet (audit et plan de sécurisation d'une autre PME fictive, avec configurations à corriger) et d'un questionnaire. Seuil de réussite interne : 70 % des critères du projet.

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Contenus sous-titrés et transcrits ; consoles reconstituées utilisables au clavier, compatibles avec l'agrandissement du texte et les thèmes à fort contraste ; journaux et configurations aussi restitués en texte (lisibles par un lecteur d'écran) ; fiches mémo et modèles accessibles. Référent handicap joignable à handicap@will-formation.com pour étudier toute adaptation (durée, supports, outils).

Tarif de la formation

Prix : **1 710 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

11 modules, 31 leçons — durée totale 26 h.

01 Positionnement et remise à niveau ciblée

1. Positionnement : bases d'administration et dossier d'Orvanne

02 Cartographier le SI et prioriser la sécurisation

1. Inventorier le parc et les logiciels
2. Cartographier les flux et les dépendances
3. Prioriser avec un référentiel d'hygiène

03 Comptes, identités et authentification

1. Gérer le cycle de vie des comptes
2. Déployer l'authentification multifacteur
3. Séparer et protéger les comptes d'administration

04 Mises à jour et gestion des vulnérabilités

1. Organiser la gestion des correctifs
2. Suivre les vulnérabilités et les avis de sécurité
3. Traiter le matériel et les logiciels en fin de support

05 Durcir et protéger les postes de travail

1. Configurer un poste de référence
2. Protection contre les codes malveillants et détection sur le poste
3. Chiffrer les postes et maîtriser les supports amovibles

06 Sécuriser le réseau

1. Segmenter le réseau de l'entreprise
2. Filtrer les flux avec le pare-feu
3. Sécuriser le Wi-Fi et les accès à distance

07 Sécuriser la messagerie et les services en ligne

1. Protéger les domaines de messagerie : SPF, DKIM, DMARC
2. Filtrer et signaler les messages malveillants
3. Sécuriser les services en ligne et le stockage partagé

08 Sauvegardes et continuité d'activité

1. Concevoir une politique de sauvegarde
2. Isoler les sauvegardes et tester la restauration
3. Plan de continuité et de reprise d'activité

09 Journaliser et détecter

1. Activer et centraliser les journaux
2. Repérer les signaux d'une compromission
3. Superviser avec des moyens proportionnés

10 Préparer et conduire la réponse à incident

1. Préparer la réponse à incident
2. Contenir, éradiquer, restaurer
3. Déclarer, communiquer, tirer les leçons

11 Prestataires, obligations et plan de sécurisation

1. Encadrer les prestataires et l'infogérance
2. Obligations : RGPD, NIS 2, clients et assurance
3. Construire et suivre le plan de sécurisation