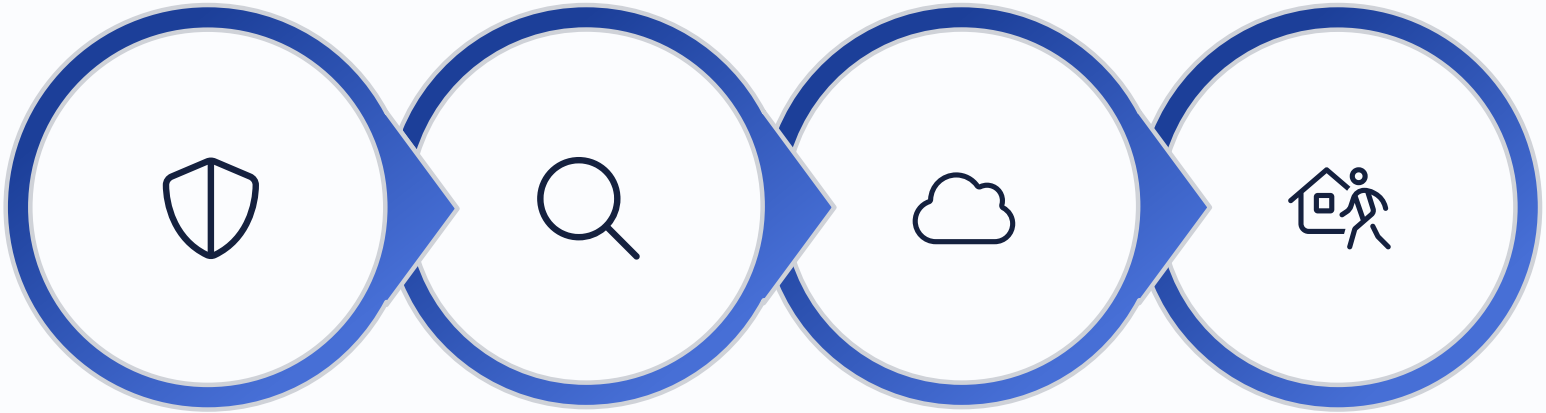
PROGRAMME DE FORMATION

CYBE-003 — Sécurité Bureautique

Une formation intensive de **14 heures** conçue pour les profils administratifs et non-techniciens, afin de maîtriser les bonnes pratiques de cybersécurité au quotidien — poste de travail, messagerie, cloud et accès distants.



Posture & Menaces | **Messagerie Sécurisée** | **Cloud & Partage** | **Accès Distants**

INFORMATIONS GÉNÉRALES

Fiche Descriptive de la Formation

Code	CYBE-003
Durée	14 heures (2 jours)
Modalité	Présentiel ou distanciel
Public cible	Profils administratifs et non-techniciens gérant des informations sensibles
Prérequis	Utilisation courante d'un poste de travail et d'une messagerie professionnelle
Effectif	6 à 12 participants
Référentiel	NIS2 — RGPD art. 32

Financement disponible

Cette formation est éligible au **Plan de Développement des Compétences (PDC)** via les OPCO suivants :

- OPCO 2i
- Atlas
- OPCO Santé
- Opcommerce
- Constructys
- Afdas
- AKTO

OBJECTIFS

Ce que vous saurez faire à l'issue de la formation

À l'issue des deux journées de formation, chaque participant sera capable de :

1	**Sécuriser son poste** Mises à jour, chiffrement du disque, antivirus et verrouillage automatique.
2	**Gérer la messagerie** Reconnaître et signaler un email malveillant, sécuriser ses communications professionnelles.
3	**Maîtriser le cloud** Distinguer cloud professionnel et personnel, gérer les droits d'accès aux fichiers partagés.
4	**Télétravail sécurisé** Utiliser un VPN correctement et appliquer les règles du travail à distance.
5	**Gérer les incidents** Appliquer la procédure de remontée d'incident en cas d'anomalie détectée.

MODULE 1

Posture et Menaces Bureautiques

DURÉE : 3H30

Menaces ciblées

Panorama des attaques visant directement le poste de travail :

- **Ransomware** — chiffrement des données contre rançon
- **Spyware** — surveillance et exfiltration silencieuse
- **Keylogger** — capture des frappes clavier

Sécurisation du poste

- Politique de mise à jour systématique
- Chiffrement du disque dur
- Verrouillage automatique de session
- Gestion des périphériques : clés USB, smartphones, imprimantes réseau

🛠️ **Atelier pratique :** Audit de sécurité de son poste de travail à l'aide d'une checklist structurée — chaque participant repart avec une évaluation personnalisée de son environnement.

MODULE 2

Messagerie Professionnelle Sécurisée

DURÉE : 3H30

Anatomie d'un email malveillant

Identification des indicateurs visuels et techniques révélateurs d'une tentative de phishing ou d'usurpation d'identité.

Spear-phishing ciblé

Exemples sectoriels concrets : finance, ressources humaines, direction — les attaques les plus sophistiquées et personnalisées.

Signature & chiffrement

Mise en œuvre de la signature numérique et du chiffrement pour les emails contenant des données sensibles.

Pièces jointes & liens

Les règles d'or pour traiter les pièces jointes et les liens hypertextes sans exposer l'organisation à un risque.

🎭 **Atelier pratique :** Identification d'emails suspects par jeux de rôle — les participants analysent des cas réels issus des bases ANSSI et CERT-FR.

MODULE 3

Stockage Cloud et Partage Sécurisé

DURÉE : 3H30

Cloud pro vs. cloud personnel

Comprendre les risques liés à l'usage de services cloud personnels (Google Drive, Dropbox…) dans un contexte professionnel, et les règles d'usage à respecter.

Gestion des droits d'accès

Partage de fichiers, attribution des permissions, et surtout **révocation des accès** lorsqu'ils ne sont plus nécessaires.

Classification des données

Quatre niveaux de sensibilité à maîtriser :

Publique	**Interne**
Confidentielle	**Sensible**

☁️ **Atelier pratique :** Audit des partages cloud de son équipe — identification des accès excessifs, des fichiers mal classifiés et des permissions à révoquer.

MODULE 4

Accès Distants et Procédures d'Incident

DURÉE : 3H30

Télétravail sécurisé

- **VPN :** fonctionnement, configuration et bonnes pratiques d'usage
- **Réseau Wi-Fi :** risques des réseaux publics et domestiques non sécurisés
- **BYOD :** règles pour les appareils personnels utilisés à des fins professionnelles
- **Double facteur :** activation et gestion de l'authentification MFA

Procédure d'incident

- Qui alerter, quand et comment signaler une anomalie
- **Détection** — identifier les signaux faibles
- **Confinement** — limiter la propagation immédiatement
- **Remédiation** — restaurer un état sain et sécurisé

📋 **Livrable remis :** Checklist de sécurisation du poste de travail + procédure d'incident personnalisée adaptée au contexte de chaque participant.

PÉDAGOGIE

Méthodes Pédagogiques

Une approche résolument **pratique et ancrée dans le réel**, combinant apports théoriques et mises en situation concrètes.

Apports théoriques

Illustrés d'incidents réels documentés par l'ANSSI et le CERT-FR.

Quiz de positionnement

Évaluation initiale en début de J1 pour adapter le niveau aux participants.

Ateliers pratiques

Audit de poste, identification d'emails suspects, audit des partages cloud.

Livrables remis

Checklist de sécurisation et procédure d'escalade incident personnalisée.

QCM d'évaluation

Validation des acquis en fin de formation avec score minimum requis.

ÉVALUATION & FORMATEUR

Validation des Acquis et Expert Formateur

Modalités d'évaluation

01

Quiz de positionnement initial

Réalisé le matin du Jour 1 pour mesurer le niveau de départ de chaque participant.

02

QCM de validation des acquis

En fin de Jour 2 — **score minimum requis : 70%** pour valider la formation.

03

Attestation individuelle

Remise à chaque participant à l'issue de la formation, nominative et certifiée.

Votre formateur

Alexandre BOIGUES

Formateur indépendant spécialisé en cybersécurité

- NDA 11 92 27843 92
- Ingénieur système et réseaux, ex-CTO
- 10 ans d'interventions en grandes entreprises
- Veille active ANSSI / CERT-FR
- Membre du réseau **CyberV**

CONTACT & TARIFS

Nous Contacter pour Organiser votre Formation

Telemach Learning

📧 **alexandre@telemach-learning.fr**

📞 **+33 6 66 88 75 63**

📍 24 Rue Chanzy, 92600 Asnières-sur-Seine

🌐 www.telemach-learning.fr

Tarifs et financement

- **Tarif intra-entreprise :** sur devis selon effectif et modalité choisie
- **Financement OPCO/PDC :** accompagnement complet dans la constitution du dossier de prise en charge

Récapitulatif rapide

14h de formation

2 jours intensifs, présentiel ou distanciel

4 modules pratiques

Poste, messagerie, cloud, accès distants

Référentiel NIS2 / RGPD

Conformité art. 32 assurée

Financement OPCO

7 OPCO partenaires éligibles