

Formation visant à sensibiliser les participants à la sécurisation des postes de travail et des applications dans un environnement professionnel



1h



e-learning



Agents, courtiers,
IOBSP et leurs
collaborateurs.



Cybersécurité

Informations générales

- Prérequis : **Sans objet**
- Niveau : **Intermédiaire**
- Délais d'accès : **Dès l'inscription**
- Modalités d'accès : **Après inscription, un mail de CGPA Campus vous invitera à rejoindre la plateforme. Le lien restera valable 2 mois.**
- Durée d'accès : **Les apprenants peuvent revoir la formation en ligne autant de fois que souhaité durant sa période d'accès.**
- Domaine : **Informatique**
- Sous-domaine : **Cybersécurité**
- Spécialité : **Sécurité informatique**
- Accès PSH : N/A
- Tarif : **offert aux sociétaires CGPA**

Objectifs de formation

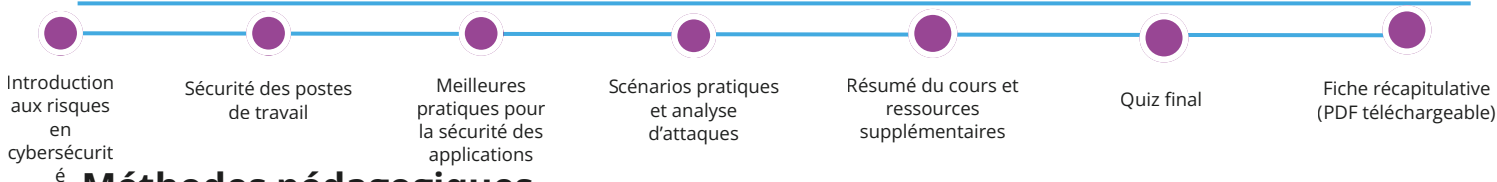
- Identifier les principaux risques liés aux postes de travail et aux applications.
- Comprendre les vecteurs d'attaque (malwares, ransomwares, vulnérabilités non corrigées, permissions abusives).
- Adopter les bonnes pratiques de configuration et de maintenance des systèmes (patching, verrouillage, principe du moindre privilège).
- Appliquer les réflexes essentiels de sécurité lors de l'installation ou de l'utilisation d'applications.
- Comprendre les scénarios d'attaque (Cyber Kill Chain, MITRE ATT&CK) pour mieux s'en prémunir.
- Renforcer la posture de sécurité grâce à des outils adaptés (EDR, chiffrement, pare-feu).
- Consolider ses acquis via un quiz final et une fiche récapitulative téléchargeable.

Critères de réussite

Une attestation est délivrée dès 70 % de bonnes réponses, téléchargeable immédiatement dans « Mes cours ». Les Apprenants seront invités à remplir un questionnaire de satisfaction permettant d'évaluer l'e-learning suivi et la fiche récapitulative sera disponible et téléchargeable sur la plateforme de formation.

Séquençage pédagogique

Nombre de parties : 7



Méthodes pédagogiques

- Apports théoriques illustrés par des scénarios concrets.
- Activités interactives : glisser-déposer, associations, QCM.
- Mises en situation basées sur des attaques réelles (phishing, keylogger, exploitation de failles).
- Fiche récapitulative.

Modalités d'évaluation

Quiz évaluation.

Formation visant à sensibiliser les participants à la sécurisation des postes de travail et des applications dans un environnement professionnel

Séquençage du module

- Seq.1 : Introduction aux risques en cybersécurité
- Seq.2 : Sécurité des postes de travail
- Seq.3 : Meilleures pratiques pour la sécurité des applications
- Seq.4 : Scénarios pratiques et analyse d'attaques
- Seq.5 : Résumé du cours et ressources supplémentaires
- Seq.6 : Quiz final
- Seq.7 : Fiche récapitulative (PDF téléchargeable)

Outils

- Plateforme LMS
- Support de cours
- Questionnaire d'évaluation QCM

Date

1er novembre 2025