

Chaîne scénarisée - Cybersécurité pour les utilisateurs

By Œil pour Œil

Formation pratique - 0j - 01h30 - Réf. 8SU

Prix : 144 CHF H.T.

NEW

Les cyberattaques se développent grâce à l'IA et menacent les entreprises et la sécurité de leurs systèmes d'informations (ou SSI). Aujourd'hui, les entreprises et organisations se doivent de se protéger contre les pirates informatiques. Cette formation ludique et accessible propose une plongée dans les menaces potentielles et vous permettra d'acquérir les bonnes pratiques en matière de SSI.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- ✓ Définir les bonnes pratiques en matière de sécurité des systèmes d'information.
- ✓ Appliquer une méthode de détection des cyber menaces.
- ✓ Reconnaître les techniques utilisées par les hackers pour obtenir des accès ou des informations.

Public concerné

Toute personne souhaitant acquérir les bonnes pratiques en matière de cybersécurité.

Prérequis

Aucun prérequis.

PARTICIPANTS

Toute personne souhaitant acquérir les bonnes pratiques en matière de cybersécurité.

PRÉREQUIS

Aucun prérequis.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Méthodes et moyens pédagogiques

Activités digitales

La structure "scénarisée" : vidéos ludiques en motion design, storytelling engageant, quiz pour évaluer les connaissances.

Tutorat

L'option tutorat propose un accompagnement personnalisé par un formateur référent ORSYS, expert du domaine. Adapté aux besoins, aux capacités et au rythme de chaque apprenant, ce tutorat combine un suivi asynchrone (corrections personnalisées d'exercices, échanges illimités par message...) et des échanges synchrones individuels. Bénéfice : une meilleure compréhension, le développement des compétences et un engagement durable dans la formation.

Programme de la formation

1 Cybersécurité et SSI

- Se protéger des menaces
- Concevoir un mot de passe fort
- Gérer ses mots de passe
- Reconnaître le phishing
- Déjouer le ransomware
- Vigilance dans le nomadisme

2 De nouvelles cybermenaces !

- Le facteur humain
- L'ingénierie sociale
- Nomadisme et Télétravail
- L'évolution du phishing
- Les réseaux sociaux
- L'importance des bonnes pratiques

3 L'intelligence artificielle au service des hackers

- L'IA au service des cyberattaquants
- Deepfakes et Voicefakes
- L'IA générative et la fuite de données
- Ingénierie sociale 2.0
- L'IA dans les malwares et ransomwares
- Se défendre face aux menaces IA

Ce programme est une création originale, conçu par les équipes pédagogiques d'ORSYS Formation. Toute reproduction, représentation, adaptation ou exploitation, totale ou partielle, sans autorisation préalable écrite d'ORSYS, est strictement interdite. ORSYS se réserve le droit d'engager toute action nécessaire à la protection de ses droits de propriété intellectuelle.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.