Date de publication : 16/06/2025

Chaîne e-learning cybersécurité

Formation pratique - 1j - 07h23 - Réf. 8CY
Prix : 190 CHF H.T.

Luttez contre les cyber-menaces grâce à notre chaîne spécialisée en cybersécurité. Découvrez les méthodes de protection des données, les techniques de prévention des attaques et les stratégies pour contrer les failles de vos infrastructures numériques. Êtes-vous prêt à devenir un expert en cybersécurité ?

Objectifs pédagogiques

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

- Connaître les mesures de protection de l'information.
- Favoriser la politique de sécurité SI de l'entreprise.
- Identifier les risques d'utilisation des outils numériques.
- Sécuriser son poste de travail.
- Mettre en œuvre le chiffrement avec BitLocker.
- Mettre en place des stratégies de groupe.
- Gérer la remontée de la clé de récupération BitLocker dans Active Directory et Azure Active Directory.
- Installer et utiliser la distribution Kali Linux.
- Analyser les vulnérabilités avec Nessus.
- Tester votre réseau avec Macchanger ou Macof.
- Comprendre le concept de Man in The Middle, ainsi que les outils d'attaque par force brute.
- Gérer la sécurisation d'un réseau WiFi.
- Déployer une solution de PKI dans l'entreprise.
- Appréhender les PKI.
- Connaître les concepts de la cryptographie.
- Comprendre le chiffrement symétrique et asymétrique.
- Utiliser des certificats et des modèles de certificats.

Public concerné

Administrateurs système et réseau et toute personne en charge de la sécurité informatique d'une entreprise.

PARTICIPANTS

Administrateurs système et réseau et toute personne en charge de la sécurité informatique d'une entreprise.

PRÉREQUIS

Connaissances sur l'utilisation d'un système Linux et Windows.

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.

Prérequis

Connaissances sur l'utilisation d'un système Linux et Windows.

Méthodes et moyens pédagogiques

Activités digitales

La structure IT : Cours enregistrés, vidéos d'expert et partages de bonnes pratiques.

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.

Pédagogie et pratique

De nombreux contenus réalisés par des formateurs suivant une démarche pédagogique rigoureuse. Durant chaque cours, des cas opérationnels sont commentés par des experts pour aider les apprenants à mettre en pratique ce qu'ils viennent d'apprendre. Afin de favoriser l'ancrage mémoriel, chaque contenu est découpé en séquences courtes de 3 à 10 minutes. Ce découpage permet un apprentissage dynamique et en toute autonomie pour chaque apprenant.

Programme de la formation

1 BitLocker, mettre en œuvre et gérer le chiffrement des postes de travail en entreprise

- Découverte de la fonctionnalité BitLocker.
- Mise en place du chiffrement avec BitLocker.

2 Kali Linux, démarrer l'analyse de la sécurité de son infrastructure

- Découverte de Kali Linux.
- Installation de Kali Linux.
- Configuration de Kali Linux.
- Découverte des vulnérabilités.
- Installation et utilisation de Nessus.
- Prise en main de Kali Linux et du réseau.
- Utilisation des outils réseau.
- Découverte de l'attaque par force brute avec Kali Linux.
- Utilisation d'outils d'attaque par force brute.
- Gestion de la sécurité WiFi.

3 PKI, mettre en œuvre et utiliser une infrastructure à clé publique en environnement Windows

- Introduction aux PKI : la cryptographie.
- Les certificats dans une infrastructure à clé publique.
- Mise en œuvre d'une PKI.
- Les modèles de certificats dans une infrastructure à clé publique.

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.