

Formation : Se protéger contre les virus et malwares en environnement Microsoft

Formation pratique - 2j - 14h00 - Réf. MAL

Prix : 1610 CHF H.T.



Cette formation détaille les virus et malwares informatiques qui dégradent le fonctionnement des ordinateurs et perturbent l'activité des entreprises. A l'issue, vous serez capable de mettre en place une démarche, de choisir les meilleures techniques et d'utiliser les bons outils pour les détecter et les éradiquer.

Objectifs pédagogiques

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

- ✓ Identifier et neutraliser les malwares ou virus
- ✓ Distinguer une infection d'un dysfonctionnement
- ✓ Utiliser les outils adéquats pour les détecter et les éradiquer
- ✓ Elaborer un plan d'action en adéquation avec les besoins de l'entreprise

Public concerné

Techniciens, administrateurs et ingénieurs systèmes/réseaux/sécurité.

Prérequis

Bonnes connaissances de la gestion de postes Windows en réseau.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant [ce test](#).

Méthodes et moyens pédagogiques

Travaux pratiques

Des stations de travail fonctionnant sous Windows 10 et Windows Server 2016 seront utilisées pour mettre en pratique les notions présentées.

PARTICIPANTS

Techniciens, administrateurs et ingénieurs systèmes/réseaux/sécurité.

PRÉREQUIS

Bonnes connaissances de la gestion de postes Windows en réseau.

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.

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.

Programme de la formation

1 Les concepts de base

- Qu'entend-on par infections virales ?
- Définition du concept de virus. Les bons outils.
- La jungle des noms (backdoor, vers, cheval de Troie, bot/botnet...).
- Principes généraux de fonctionnement des menaces.
- Les vecteurs d'infection les plus répandus.
- Désactivation et contournement des sécurités.

Travaux pratiques

Analyse d'une infection (backdoor, rootkit...). Le spyware et le phishing.

2 Comment se protéger ? L'antivirus et le Firewall

- Les principes de fonctionnement.
- Les types de détection (par signature, heuristique, comportementale...).
- Les Packers (UPX, FSG, Upack, Armadillo, Themida...).
- Les fausses alertes.
- Présentation du Firewall. Les bons outils.
- Que peut-il détecter ?
- Quelles sont ses limites ?

Travaux pratiques

Test de détection avec les différents types et contournement d'un Firewall.

3 Mécanismes d'infection

- Le fonctionnement des programmes.
- La relation avec les DLL.
- Les injections de code.
- Comment détecter une infection au démarrage ? Les bons outils.
- Rappel du démarrage de Windows.
- Les outils appropriés.
- Les infections et la base de registre.

Travaux pratiques

Exemple d'injection virale. Simulation d'un code malicieux en phase de démarrage et techniques d'éradication.

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'émergence 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.

4 Identifier pour mieux éradiquer

- L'importance de bien identifier la menace.
- Utiliser l'outil le plus approprié : Windows Defender, les outils concurrents.
- Eradiquer "l'éternel retour".
- Supprimer les résidus inactifs.

Travaux pratiques

Utilisation de scripts pour contrer les infections. Comment identifier les sources d'infection ? Eradiquer sans formater.

5 Prévenir plutôt que guérir

- Sensibiliser les utilisateurs.
- Les procédures à mettre en place.
- Choisir ses systèmes de sécurité.
- Les sauvegardes et les points de restauration.
- Choisir les bons outils.
- Les solutions du marché et l'Appliance antivirus.

Travaux pratiques

Identifier les étapes d'un plan d'action à mettre en place en entreprise.

Dates et lieux

CLASSE À DISTANCE

2026 : 11 juin, 22 oct.