+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Mécanisme d’infection des malwares et les contre-mesures pour Windows

Plus de 75% de la formation est constituée d'exercices pratiques et de mise en situation.

À qui s'adresse la formation ?

- Techniciens, administrateurs et ingénieurs systèmes/réseaux/sécurité.

+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Informations clés

Jours de formations	**2**
Lieu	**Présentiel / Distanciel**
Horaires	**9h - 12h30 / 13h30 - 17h00.**
Prix global	**1290 €**
Eligibilité aux OPCO	**Oui**
Eligibilité aux CPF	**Lien CPF**
Langue	**Français**
Vidéos	**Non**
Durée de l'examen	**Selon la certification demandée**

+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Objectifs de la formation

- Identifier et neutraliser les malwares sous Windows.
- Distinguer une infection d'un dysfonctionnement.
- Utiliser des outils adéquats pour détecter et éradiquer les malwares.
- Élaborer un plan d'action adapté aux besoins de l'entreprise.

Approche pédagogique

Cette formation comporte plusieurs ateliers pratiques sur des environnements techniques. Les sessions "A distance" sont réalisées avec un outil de visioconférence, permettant au formateur d'adapter sa pédagogie.

L'évaluation se fait en continue au fils des travaux pratiques.

Prérequis

- Connaissances en OS Windows.
- Capacité en scripting sous Windows.
- Accès administrateur sur un ordinateur.

+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Programme de la formation

Jour 1

Compréhension des Malwares et Réponse Initiale

Matin : Les concepts de base et mécanismes d'infection

- Introduction aux malwares : définitions, types et vecteurs d'infection.
- Fonctionnement des programmes malveillants et relation avec les DLL.
- Techniques d'injection de code et détection au démarrage.

Après-midi : Travaux pratiques

- Analyse et simulation d'infections (backdoor, rootkit, spyware, phishing).
- Exercices sur les techniques d'injection virale et d'éradication.

Jour 2

Stratégies de Neutralisation et Prévention

Matin : Identifier et éradiquer les malwares

- Stratégies d'identification et d'éradication des malwares.
- Utilisation d'outils de sécurité spécifiques à Windows.

Après-midi : Travaux pratiques et prévention

- Mise en pratique des stratégies d'identification et d'éradication.
- Sensibilisation des utilisateurs, procédures de sécurité, sauvegardes et points de restauration.