ALYF

Windows 10 - Sécurité

Référence : W10-SEC
Durée : 3 jours (21h)
Tarif : 2400 €
Date à planifier

Certification : Aucune
Code CPF Unique : Aucun - **Code Certif Info :** Aucun

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel.

Le formateur alterne entre méthode* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en œuvre sont :

- Ordinateurs Mac ou PC, connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

** ratio variable selon le cours suivi*

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

A l'issue de ce stage vous serez capable de :

- Sécuriser un poste de travail sous Windows 10.

Public :

Administrateurs systèmes, administrateurs SSI.

Prérequis :

Connaître l'administration de Windows.

Les plus de la formation :

Un guide de recommandations et de bonnes pratiques sera fourni, en sus du support de cours.

Cette formation :

- bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.
- est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par ALYF

Programme

Jour 1

- **Les nouveautés**

Les changements

Notion de malwares

Analyse de risque

- **Faille physique**

Contre-mesure

- **Gestion des comptes**

Comprendre UAC (User Account Control)

Exemples de travaux pratiques (à titre indicatif)

MFA user (Multi-Factor Authentication)

UAC

- **Gestion des droits**

FAT (File Allocation Table)

NTFS (New Technology File System)

ReFS

AGDLP (Account, Global, Domain Local, Permission)

Exemples de travaux pratiques (à titre indicatif)

NTFS et héritage

- **Les outils de base en pratique**

Observateur d'évènements

MSH (Microsoft Command Shell)

PowerShell

MMC

Sysinternal

Exemples de travaux pratiques (à titre indicatif)

Clé USB des outils de base

Jour 2

- **Protection du réseau**

Les types d'attaques

Protocoles et requêtes dans Windows

NBT-NS, LLMNR, WPAD, IPv6, mDNS

Se protéger

Surveillance réseau

Notion du "packet filtering"

Exemples de travaux pratiques (à titre indicatif)

Exercice Wireshark

- **Sécurité des applications**

Windows Defender

ATP vs EMET

Protection arbitraire du code

Exemples de travaux pratiques (à titre indicatif)

Exercice Exploit Guard

- **Chiffrements**

Chiffrement des dossiers et des fichiers

BitLocker :

- Avec TPM
- Sans TPM

IPsec

Règles du pare-feu

Jour 3

- **Sauvegarde et restauration**

Types de sauvegardes dans Windows 10

Nouvelle version

Sauvegarde automatique

Fréquence des sauvegardes

Image système

Restauration

Nouvelle version

Restaurer image système

- **Last Update may-2019 19h1 1903**

Nouveautés de Windows 10, version 1903

StartMenuExperience

Update

L'Assistant Stockage 1903

Windows Defender

Ordinateur virtuel (Windows Sandbox)

Subsystem for Linux

Partage des mises à jour

Sécurité du navigateur

- **Exemples de travaux pratiques (à titre indicatif)**

Créer une image système sécurisée avec obligation :

- *UEFI sécurisé*
- *MFA*
- *Process Explorer*
- *NO : NBT-NS, LLMNR, WPAD, IPv6, mDNS*
- *Protection arbitraire du code*
- *Exploit Guard*
- *BitLocker*
- *Vérifier les signatures*
- *Logiciel*
- *DLL (Dynamic Link Library)*
- *Driver*

- **Pare-feu**

Profils

SUIVI DE L'EXECUTION ET EVALUATION DES RESULTATS

> Feuilles de présence

> Questions orales ou écrites(QCM)

> Mises en situation

> Formulaires d'évaluation de la formation

> Certificat de réalisation de l'action de formation