Développez vos talents
Certifiez vos compétences

Windows 10

Windows 10 - Sécurité

3 jours (21h00) | ★★★★½ 4,6/5 | W10-SEC | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Systèmes › Windows 10

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

- Sécuriser un poste de travail sous Windows 10.

Niveau requis

Connaître l'administration de Windows.

Public concerné

Administrateurs systèmes, administrateurs SSI.

Cette formation :

- 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 M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), 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.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

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

Pare-feu

- Profils
  - 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*

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 ou une certification (M2i ou éditeur)

Les + de la formation

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