Sécurité défensive

# Sécurité du poste client Windows

2 jours (14h00) | ★★★★½ 4,6/5 | SEC-CLI | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel



*Contenu mis à jour le 13/10/2023. Document téléchargé le 07/06/2024.*

## Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Sécuriser un poste de travail sous Windows
- Mettre en oeuvre les bonnes pratiques
- Expliquer les tenants et les aboutissants d'un durcissement client.

## Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

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 oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains 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

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

## Prérequis

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.

# Programme

## Tour d'horizon des risques

- Vue d'ensemble des risques
- Méthodes d'analyses de risques
- Evaluer sa maturité SSI
- Vue d'ensemble des recommandations

## Gérer un projet de durcissement

- Comprendre les différents protocoles existants
- Comprendre les notions d'identité et de données
- Les risques sont-ils tous bons à être gérés ?
- Cas concrets d'entreprises
- Communications associées

## Durcissements Hardware

- Principe de RoT (Root of Trust) et de PC Secured-core
- Windows Defender System Guard
- Compréhension SMM
- Gestion TPM
- Mise en oeuvre du VBS, HVCI, du stack renforcé, du KDMA
- Mise en oeuvre du System Guard Launch

## Sécurité du système

- Vue d'ensemble des pratiques de durcissement
- Sécurisation du Boot
- Mise en oeuvre du DHA (Device Health Attestation)
- Protection contre les menaces
- Mise en oeuvre de la sécurité des périphériques

## Microsoft Defender

- Vue d'ensemble des outils Microsoft Defender On-Premise et Cloud
- Mise en oeuvre de Windows Defender Security Center, Antivirus, SmartScreen, Endpoint

## Sécurisation du réseau

- Gestion des protections réseaux
- Gestion des sécurités Wi-Fi
- Mise en oeuvre du TLS

- Mise en oeuvre de l'EAP
- Configuration avancée du firewall
- Introduction au VPN, Always On VPN, Direct Access
- Durcissement du SMB

## Durcissement des données

- Chiffrement de disques et de fichiers avec Bitlocker, EFS et PDE (Personal Data Encryption)
- Introduction et mise en oeuvre de Windows Information Protection
- Introduction aux technologies Azure

## Gestion des périphériques

- Configuration des stratégies de sécurité
- Gestion des audits de sécurité
- Gestion des events de sécurité
- Gestion du mode secured-core lock
- Gestion du mode Kiosk

## Contrôle des applications

- Comprendre l'UAC (User Account Control)
- Mise en oeuvre de Windows Defender Application Control et du VBS
- Intégration de Smart App Control
- Configuration de Windows Defender Application Guard
- Introduction aux conteneurs : tenants et aboutissants
- La sandbox en détails

## Protection de l'identité

- Bonnes pratiques de protection de l'identité
- Mise en oeuvre du "passwordless", du MFA (Multi-Factor Authentication), de l'authentification par certificat / Smartcard
- Gestion des stratégies de blockages
- Mise en oeuvre de LAPS
- Gestion des contrôles d'accès
- Sécurisations des comptes locaux et comptes de domaines
- Mise en oeuvre de Windows Defender Credential Guard

## La sécurité avec le Cloud

- Tenants, aboutissants et limites d'une intégration Cloud au durcissement
- Vue d'ensemble des outils Azure associés
- Intégration des agents Intune
- Mise en oeuvre des bonnes pratiques Intune
- Vue d'ensemble des outils d'audit et de préconisations
- Intérêt de l'AutoPath et de l'Autopilot

## Bonnes pratiques

- Vue d'ensemble des bonnes pratiques et référentiels
- Mise en oeuvre d'actions préconisées
- Mise en oeuvre du Security Compliance Toolkit et du MBSA (Microsoft Baseline Security Analyzer)

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

## Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques

– Et, en fin de formation, par un questionnaire d'auto-évaluation

## Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

## Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.