Plan de cours N° : 1357
Durée : 3 jours (21h)

HARDENING WINDOWS
Sécurisation des postes et serveurs Windows

PARTICIPANTS / PRE-REQUIS
Administrateurs systèmes Windows, Responsables sécurité informatique, Techniciens systèmes et réseaux, Consultants IT

Connaissances de base en administration Windows Server ou Windows 10 ou 11. Maîtrise des notions fondamentales de sécurité informatique

OBJECTIFS PEDAGOGIQUES
Définir les concepts de base du hardening, y compris les objectifs, les enjeux et les menaces courantes. Expliquer les modèles de menace tels que la cyber kill chain et MITRE ATT&CK, ainsi que les guides de durcissement (ANSSI, CIS Benchmark, STIG, etc.). Mettre en oeuvre des stratégies de sécurité locales pour durcir un poste isolé, y compris la gestion des comptes, la configuration du pare-feu Windows et la désactivation des services non essentiels. Evaluer la conformité d'un poste ou d'un serveur en utilisant des outils d'audit. Implémenter des mesures de durcissement spécifiques pour des rôles serveur, y compris un contrôleur de domaine, un serveur de fichiers et un serveur RDS, en utilisant des outils avancés comme ATA et Defender ATP.

MOYENS PEDAGOGIQUES
Tour de table au début de chaque formation pour définir les objectifs de chaque participant,
Alternance entre apports théoriques (en moyenne 30%) et exercices pratiques (en moyenne 70%),
Utilisation de cas concrets issus de l'expérience professionnelle de nos formateurs,
Remise d'un support de cours,
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS
Positionnement préalable oral ou écrit,
Evaluation des acquis tout au long de la formation par des exercices de synthèse,
Attestation de stage remise à chaque apprenant, avec son niveau d'acquisition pour chaque objectif pédagogique,
Feuille de présence signée par demi-journée,
Questionnaire de satisfaction pour évaluer la qualité de l'enseignement,
En option : passage certification possible selon les thématiques

MOYENS TECHNIQUES EN PRESENTIEL
Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc

MOYENS TECHNIQUES DES CLASSES A DISTANCE
Grâce à un logiciel comme Teams, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Nous vous conseillons très fortement l'utilisation de votre webcam et de disposer d'un double écran.
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 04.76.41.14.20..

ORGANISATION
Les cours ont lieu de 9h00-12h30 13h30-17h00 (adaptable à la demande).

PROFIL FORMATEUR
Nous recrutons méticuleusement nos formateurs selon 3 critères : expertise, pédagogie et agilité.

ACCESSIBILITE
Les personnes atteintes de handicap souhaitant suivre nos formations sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités d'organisation.

MISE A JOUR
12/05/2025

Plan de cours N° : 1357
Durée : 3 jours (21h)

HARDENING WINDOWS
Sécurisation des postes et serveurs Windows

INTRODUCTION ET PRINCIPES DE BASE
- Introduction au hardening
  - Objectifs
  - Enjeux
  - Menaces courantes
- Modèles de menace
  - Cyber kill chain
  - MITRE ATT&CK
- Présentation des guides de durcissement
  - ANSSI
  - CIS Benchmark
  - STIG…
- Inventaire et priorisation des machines
- Stratégie de mise en oeuvre progressive

DURCISSEMENT DE L'OS (POSTE ISOLE)
- Configuration locale via stratégies de sécurité
- Gestion des comptes
  - Suppresion comptes par défaut
  - Verrouillage
  - Mot de passe
- Configuration du pare-feu Windows
- Durcissement des services
  - Désactivation des services non essentiels
- Surveillance des connexions et de l'activité locale (journaux d'événements)

HARDENING VIA GPO ET ACTIVE DIRECTORY
- Centralisation du durcissement avec GPO
- Paramètres de sécurité (Audit, UAC, LAPS…)
- Restrictions logicielles (SRP, AppLocker)
- Gestion des ports et protocoles autorisés
- Gérer les droits d'administration (principe du moindre privilège)

MISE A JOUR, ANTIVIRUS ET JOURNALISATION
- Windows Update, WSUS et stratégie de patch management
- Configuration de Microsoft Defender AV / Exploit Guard
- Activation et configuration de la journalisation avancée (Event Forwarding, Sysmon)
- Surveillance via Windows Security Logs

OUTILS D'AUDIT ET VERIFICATION
- Utilisation de Microsoft Security Compliance Toolkit (anciennement SCM)
- Outils de vérification CIS-CAT, Lynis, Baseline Security Analyzer
- Scripts PowerShell pour audit et reporting
- Vérification de conformité et gestion des écarts
- Introduction à la gestion centralisée (Intune, Defender for Endpoint)

CAS PRATIQUES AVANCES ET DURCISSEMENT DES ROLES SERVEUR
- Focus : Durcissement d'un contrôleur de domaine, d'un serveur de fichiers, d'un serveur RDS
- Mesures spécifiques aux environnements serveurs
- Introduction à l'ATA (Advanced Threat Analytics) / Defender ATP
- Bonnes pratiques post-déploiement (documentation, supervision, revues régulières)