

Formation Durcissement (hardening) des systèmes Windows

Réf. SF33616

Apprenez à transformer vos postes et serveurs Windows en environnements véritablement résistants face aux cyberattaques modernes !

3 j Durée	2 700 € HT Inter / participant	6 600 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Identifier et prioriser les principales surfaces d'attaque d'un poste ou serveur Windows et formaliser des mesures de durcissement adaptées
- ✓ Configurer la sécurité d'un poste Windows 10/11 de façon à réduire la surface d'exposition et bloquer le trafic non autorisé
- ✓ Mettre en œuvre via les stratégies de groupe (GPO) un jeu cohérent de paramètres de durcissement pour des machines Windows
- ✓ Déployer une stratégie de gestion des correctifs et de protection antivirus/EDR pour un petit parc Windows en configurant Windows Update/WSUS, Microsoft Defender et les alertes de sécurité
- ✓ Auditer le niveau de conformité d'un système Windows durci en utilisant Microsoft Security Compliance Toolkit, les journaux d'événements et des scripts PowerShell

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux

Prérequis Maîtrise de base de l'administration Windows client et server, connaissances fondamentales des réseaux TCP/IP et des principes de cybersécurité, notions d'Active Directory et de gestion des GPO, ainsi qu'une pratique de PowerShell.

Programme détaillé

Panorama des menaces et bases du hardening Windows

Rappels cybersécurité : modèles d'attaque (Cyber Kill Chain, MITRE ATT&CK) appliqués à Windows
Notions de surface d'attaque, d'exposition et de criticité métier
Panorama des référentiels de durcissement (ANSSI, CIS Benchmarks, STIG, Microsoft Security Baselines)
Outils d'inventaire et de découverte : Nmap, PowerShell, scripts d'inventaire WMI/WinRM
Méthode de priorisation : quick wins vs chantiers structurants, approche par rôles (poste utilisateur, serveur membre, contrôleur de domaine)
Mise en place de l'environnement de labo Windows pour les travaux pratiques

Activités pratiques :

Construire la cartographie simplifiée d'un petit SI Windows (postes, serveurs, DC) à partir de scans Nmap et d'un inventaire PowerShell
Identifier et lister au moins 10 surfaces d'attaque potentielles sur une machine Windows de labo
Élaborer une première liste priorisée de mesures de durcissement à partir d'un benchmark CIS ou ANSSI

Durcissement local des postes Windows 10/11

Stratégies de sécurité locale : secpol.msc, Local Security Policy, gestion des droits utilisateurs et UAC
Politiques de mots de passe, verrouillage de session, gestion des comptes locaux (suppression des comptes inutiles, renommage de l'administrateur, comptes invités)
Gestion des services Windows : analyse, désactivation des services non essentiels, configuration des fonctionnalités facultatives
Configuration du pare-feu Windows Defender : profils, règles entrantes/sortantes, filtrage par programme, port et adresse IP
Contrôle des accès distants (RDP, WinRM, SMB, partage de fichiers/imprimantes), protection des périphériques amovibles et introduction au chiffrement (BitLocker)
Bonnes pratiques de durcissement pour un poste isolé (laptop nomade vs poste fixe)

Activités pratiques :

Durcir un poste Windows 10/11 de labo à partir d'une checklist fournie (comptes, services, RDP, pare-feu) et documenter les changements réalisés
Réaliser un avant/après de l'exposition réseau du poste (scan de ports, tests d'accès distants) et analyser les différences
Simuler un scénario d'attaque simple (compte faible, service exposé) puis vérifier comment les mesures de durcissement le bloquent

Hardening centralisé via GPO et Active Directory

Rappels Active Directory : OU, héritage des GPO, filtrage de sécurité et WMI
Modélisation d'un jeu de GPO de sécurité par type de machine (postes utilisateurs, serveurs membres, contrôleurs de domaine)
Paramètres clés de GPO : politiques de mots de passe/déverrouillage, restrictions d'accès local, sécurité du réseau, configuration du pare-feu Windows
Restrictions logicielles : Software Restriction Policies vs AppLocker (modes, règles, scénarios d'usage)
Hardening des comptes et rôles privilégiés : comptes administrateurs locaux, comptes de service, groupes protégés, LAPS, séparation des comptes d'admin
Bases de la sécurisation des contrôleurs de domaine (services exposés, canaux sécurisés, logs critiques)

Activités pratiques :

Créer une structure d'OU et déployer des GPO de durcissement distinctes pour postes utilisateurs, serveurs membres et DC dans un domaine de labo
Mettre en place une politique AppLocker ou SRP bloquant l'exécution d'applications non approuvées et vérifier son effet sur un poste test
Déployer LAPS ou une solution équivalente sur le labo et démontrer la rotation et la protection des mots de passe administrateur local

Patch management, Microsoft Defender et journalisation avancée

Mise à jour Windows : Windows Update for Business, WSUS, anneaux de déploiement, gestion des redémarrages et des fenêtres de maintenance
Présentation des composants Microsoft Defender (AV, Exploit Guard, Attack Surface Reduction, SmartScreen) et intégration possible avec Defender for Endpoint
Paramétrage des exclusions, scans programmés, politiques d'alerte et de remédiation
Architecture des journaux d'événements Windows (Security, System, Application, Microsoft-Windows-*), bonnes pratiques de rétention
Collecte centralisée : Windows Event Forwarding, introduction à Sysmon (événements détaillés de processus, réseau, fichiers)
Premiers pas vers l'intégration SIEM (ex. Sentinel, solution open source) : formats, connecteurs, corrélation basique

Activités pratiques :

Configurer les paramètres Windows Update/WSUS pour un groupe pilote de machines et simuler un cycle complet de déploiement de correctifs
Déployer et paramétrer Microsoft Defender AV et quelques règles d'Attack Surface Reduction sur des postes de labo, puis tester des scénarios d'exécution bloquée
Installer Sysmon avec une configuration type, générer des événements (lancement de script, accès réseau) et analyser les journaux collectés via Event Viewer ou un collecteur central

Audit de conformité, automatisation PowerShell et plan d'actions

Présentation et positionnement de Microsoft Security Compliance Toolkit (SCT) et des benchmarks CIS/CIS-CAT
Choix et adaptation d'une baseline de sécurité Windows en fonction du contexte de l'organisation
Scripts PowerShell d'audit : vérification des services, des paramètres de registre, des correctifs installés, des GPO appliquées
Interprétation des résultats d'audit : scores de conformité, écarts critiques vs tolérables, alignement avec les risques métier
Construction d'un plan d'actions : quick wins, roadmaps de durcissement, gouvernance et mise à jour continue des baselines

Activités pratiques :

Exécuter SCT ou un benchmark CIS sur une machine Windows de labo, analyser le rapport généré et identifier les écarts les plus critiques
Écrire ou adapter un script PowerShell qui vérifie au moins 10 contrôles de durcissement (services, ports, GPO, version de patch) et exporter les résultats en CSV/HTML
Réaliser, en sous-groupes, un mini rapport d'audit et un plan de remédiation priorisé pour l'environnement de labo, puis le présenter à l'oral

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Administration Windows : 4,9/5 — 15 avis

Tom K. — Merci beaucoup pour cette formation, Mr Roux ! Votre niveau d'expertise est vraiment top. Le sujet étant passionnant mais certains TP assez complexes, est-ce que les enregistrements du...

Bruno G. — Excellente formation : Répond à mes attentes. Supports de cours excellents et en nombre Pédagogie parfaite Compétences pointues de Fabien disponibilité permanente Machine virtuelle parfaite sans bug et...

Votre formateur

Fabien R. — Formateur Windows

Fabien intervient sur des formations portant sur l'administration des environnements Windows. Parmi les formations qui lui sont confiées figurent notamment « VBScript » et « PowerShell ». Son activité de...

Ils nous font confiance

Cette année notre filière Administration Windows a accompagné plus de 45 entreprises dont :

INETUM ARPEGE CEGEDIM CIMPA SAS INETUM SOFTWARE FRANCE SCC FRANCE SAS SOPRA STERIA I2S ALCATEL SUBMARINE NETWORKS
ALTYN APSIDE TOULOUSE +35 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com