[TECH03]

- **Objectifs**
  - **Comprendre les enjeux du durcissement d'une infrastructure Windows**
  - **Savoir réaliser un état des lieux des vulnérabilités et appliquer les bonnes pratiques**
  - **Identifier et corriger les vulnérabilités**
  - **Garantir la conformité aux standards de sécurité et aux exigences réglementaires**

- **Public visé**
  - Tout professionnel impliqué dans la gestion ou la sécurisation du SI

- **Prérequis**
  - Connaissances de base en administration Windows Server (notamment Active Directory)
  - Notions fondamentales en cybersécurité et gestion des identités

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Cyberdefense

Mettre en place le durcissement d'une infrastructure Windows

Programme de formation

- **Introduction et enjeux du durcissement**
  - Les risques et vulnérabilités d'une infrastructure Windows
  - Le cadre réglementaire associé

- **Analyse préalable et audit de sécurité**
  - État des lieux de l'environnement Windows
  - Outils d'audit et de scan de vulnérabilités (Microsoft Security Compliance Toolkit, Nessus, etc.)
  - Identification des points faibles et priorisation des actions

- **Stratégie de sécurité et configuration**
  - Mise en place et gestion des stratégies de groupe (GPO)
  - Configuration des paramètres de sécurité locaux et de domaine
  - Sécurisation des comptes utilisateurs et des groupes
  - Gestion des mots de passe et des politiques de verrouillage

- **Sécurisation des services et composants Windows**
  - Désactivation ou sécurisation des services non nécessaires
  - Configuration du pare-feu Windows et des règles avancées
  - Sécurisation des protocoles
  - Mise en place de l'authentification forte

- **Gestion des mises à jour et correctifs**
  - Stratégies de déploiement des mises à jour Windows
  - Automatisation des correctifs de sécurité
  - Vérification de la conformité des patchs

- **Sécurisation des accès et des ressources**
  - Mise en place de contrôles d'accès Segmentation du réseau et VLAN
  - Mise en œuvre de VPN et de solutions d'accès sécurisé
  - Gestion des accès à distance et à l'aide de RDP

- **Surveillance, audit et réponse aux incidents**
  - Mise en place de la journalisation et de la surveillance
  - Utilisation des outils associés
  - Détection et réponse aux incidents de sécurité
  - Plan de reprise d'activité et sauvegarde sécurisée

[TECH03] Mettre en place le durcissement d'une infrastructure Windows

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Exercices pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	Français / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).