[TECH02]

- **Objectifs**
  - **Comprendre les enjeux de sécurité, les vulnérabilités et les risques liés à Active Directory**
  - **Déployer des mesures de protection avancées (sécurisation des comptes, audit, segmentation)**
  - **Savoir détecter et répondre aux incidents liés à Active Directory**
  - **Maintenir une posture de sécurité conforme aux exigences réglementaires**

- **Public visé**
  - Tout professionnel impliqué dans la gestion et la sécurisation des infrastructures Active Directory

- **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

Renforcer la sécurisation de l'Active Directory

Programme de formation

- **Introduction à la sécurisation d'Active Directory**
  - Rôle et architecture d'Active Directory
  - Enjeux de sécurité spécifiques au secteur de la santé
  - Cadre réglementaire (RGPD, recommandations CNIL, HDS le cas échéant)

- **Analyse des vulnérabilités et risques**
  - Identification des vecteurs d'attaque (pass-the-hash, escalade de privilèges, etc.)
  - Cartographie des risques liés à AD, outils d'audit et de détection

- **Bonnes pratiques et stratégies de sécurisation**
  - Gestion des comptes et des privilèges (principes du moindre privilège)
  - Sécurisation des contrôleurs de domaine
  - Mise en œuvre de stratégies de mot de passe et d'authentification forte
  - Configuration des GPO pour renforcer la sécurité
  - Segmentation et isolation des services

- **Sécurisation avancée et détection**
  - Mise en place de l'audit avancé (journaux, alertes)
  - Détection des comportements suspects
  - Utilisation d'outils de monitoring (Microsoft Defender for Identity, SIEM)

[TECH02] Renforcer la sécurisation de l'Active Directory

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Exercices pratiques (plan de sécurisation pour un environnement AD, analyse de logs et détection d'incidents, exercices de sécurisation et de restauration)
- 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).