



<b>Objectifs</b>	Maîtriser les techniques de sécurité avancée sous Windows Server 2019/2022
<b>Participants</b>	Administrateurs systèmes - Ingénieurs réseaux - Techniciens IT
<b>Prérequis</b>	Connaissances de base en administration de systèmes et réseaux
<b>Moyens pédagogiques</b>	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation.
<b>Méthodes pédagogiques</b>	Exposés interactifs et démonstrations - Ateliers individuels et en groupe - Échanges d'expériences et de bonnes pratiques
<b>Type de formation</b>	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
<b>Tarif inter-entreprise</b>	3250 € HT
<b>Durée</b>	5 jour(s) - 35 heure(s)
<b>Modalités et délais d'accès</b>	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

**Code : NCI\_10T4MPA**

**Mis à jour le : 25 mars 2026**

### **Programme :**

#### **Introduction à la sécurité avancée**

Présentation des concepts de sécurité avancée  
Comparaison des fonctionnalités de sécurité entre Windows Server 2019 et 2022  
Architecture de sécurité de Windows Server

Gestion des conformités et des audits  
Bonnes pratiques de gouvernance

#### **Gestion des identités et des accès**

Azure Active Directory et intégration hybride  
Authentification multi-facteurs (MFA)  
Gestion des accès conditionnels

#### **Sécurité des applications et des workloads**

Sécurisation des applications web et des API  
Gestion des conteneurs et des microservices  
Sécurisation des workloads avec Azure Security Center

#### **Sécurisation des réseaux**

Configuration avancée des pare-feu et des groupes de sécurité réseau (NSG)  
Sécurisation des connexions VPN et des réseaux virtuels  
Protection contre les attaques réseau

#### **Protection des données**

Chiffrement des données au repos et en transit  
Utilisation de BitLocker et de Windows Information Protection  
Gestion des clés avec Azure Key Vault

#### **Surveillance et gestion des menaces**

Utilisation de Windows Defender Advanced Threat Protection (ATP)  
Configuration et gestion des alertes de sécurité  
Analyse des journaux et des événements de sécurité

#### **Conformité et gouvernance**

Mise en œuvre des politiques de sécurité (GPO)