

## Formation Active Directory : Sécurisation

<b>Durée :</b>	3 jours
<b>Public :</b>	Administrateurs systèmes Windows
<b>Pré-requis :</b>	Maîtrise de l'administration des systèmes sous Windows Server et Active Directory
<b>Objectifs :</b>	Concevoir une architecture Active Directory sécurisée - Mettre en œuvre un plan d'action de gestion de risques liés à Active Directory - Mettre en place des mécanismes de protection d'Active Directory - Gérer les identités hybrides - Gestion des sinistres et des solutions PCA/PRA pour Active Directory
<b>Sanction :</b>	Attestation de fin de stage mentionnant le résultat des acquis
<b>Taux de retour à l'emploi:</b>	Aucune donnée disponible
<b>Référence:</b>	WIN102128-F
<b>Note de satisfaction des participants:</b>	Pas de données disponibles

### Sécuriser les infrastructures Windows Server locales et hybrides

Implémenter des groupes de sécurité réseau et des machines virtuelles IaaS Windows  
Implémenter le durcissement réseau adaptatif  
Implémenter le pare-feu Azure et des machines virtuelles IaaS Windows  
Implémenter un pare-feu Windows avec des machines virtuelles IaaS Windows Server  
Choisir la solution de filtrage appropriée  
Mise en œuvre de l'ADFS  
Déployer et configurer le Pare-feu Azure à l'aide du portail Azure  
Capturer le trafic réseau avec Network Watcher  
Journaliser le trafic réseau à destination et en provenance d'une machine virtuelle à l'aide du portail Azure

**Atelier : Synchronisation AD / Azure AD, configuration ADFS et paramétrage des outils de sécurité, d'audit et de reporting Azure**

### Sécurité des serveurs Windows

Confiance zéro et Windows  
Sécurité matérielle  
Processeur de sécurité Microsoft Pluton  
Microsoft Pluton en tant que TPM  
Utilisation du Module de plateforme sécurisée (TPM) par Windows  
Paramètres de stratégie de groupe du Module de plateforme sécurisée (TPM)  
Sauvegarder les informations de récupération du module de plateforme sécurisée (TPM) dans AD DS

Lancement sécurisé de System Guard et protection SMM  
Activer la protection basée sur la virtualisation de l'intégrité du code  
Sécuriser le processus de démarrage de Windows  
Chiffrement et gestion des certificats  
Protection contre les virus et menaces  
Paramètres de stratégie de sécurité  
Audit de sécurité  
Chiffrement et protection des données  
Disques durs chiffrés et BitLocker : Déploiement et administration  
Services de domaine Active Directory  
Déploiement de base de BitLocker  
Activer le déverrouillage réseau avec BitLocker  
Lignes de base de Sécurité Windows  
Boîte à outils de conformité de la sécurité  
Remplacer les options de traitement des préventions pour appliquer des stratégies de sécurité liées à l'application  
Utiliser Windows Event Forwarding pour optimiser la détection d'intrusion  
Bloquer les polices non approuvées dans une entreprise

### **Atelier : Paramétrage des composants de sécurité sur un serveur Windows**

#### **Protection des informations Windows (WIP)**

Créer et déployer une stratégie WIP dans Microsoft Intune  
Associer et déployer une stratégie VPN pour WIP dans Microsoft Intune  
Créer et vérifier un certificat d'Agent de récupération de données (DRA) EFS  
Déterminer le contexte d'entreprise d'une application en cours d'exécution dans le WIP  
Renforcement de la sécurité à l'aide du NPS  
Créer une stratégie WIP à l'aide de Microsoft Configuration Manager  
Créer et déployer une stratégie WIP dans le gestionnaire de configuration  
Tâches et paramètres requis pour activer la fonctionnalité WIP  
Limitations pendant l'utilisation de WIP  
Comment collecter les journaux d'événements d'audit WIP  
Recommandations d'ordre général et meilleures pratiques pour WIP  
Applications compatibles à utiliser avec la fonctionnalité WIP

### **Atelier : Installation ,configuration et paramétrage d'un serveur NPS. Paramétrage des stratégies WIP sur Azure**

#### **Sécurité des applications**

Contrôle d'application Windows Defender et protection basée sur la virtualisation d'intégrité du code  
Contrôle d'application Windows Defender  
Microsoft Defender Application Guard

### **Atelier : Paramétrage des services Defender**

#### **Bac à sable Windows**

Architecture Bac à sable Windows  
Configuration du Bac à sable Windows  
Vue d'ensemble de Microsoft Defender SmartScreen  
Protection renforcée contre le hameçonnage dans Microsoft Defender SmartScreen  
Configurer S/MIME pour Windows

Prévention du vol des informations d'identification  
Gestion de la DLP

### **Atelier : Mise en place d'un bac à sable Windows**

#### **Sécurité des utilisateurs et identité sécurisée**

Chargement de certificat d'entreprise  
Protéger les informations d'identification de domaine dérivées avec Credential Guard  
Fonctionnement de Credential Guard  
Configuration requise de Credential Guard  
Gérer Credential Guard  
Limites de protection de Credential Guard  
Protéger les informations d'identification du Bureau à distance avec Remote Credential Guard  
Paramètres de clé de Registre et de stratégie de groupe de contrôle de compte d'utilisateur  
Mise en œuvre de l'ADCS et sa synchronisation avec Azure pour la sécurité de l'ADDS.

### **Atelier : Paramétrage d'un serveur Windows avec le Credential Guard, Installation et configuration de l'ADCS pour la sécurisation de l'ADDS**

#### **Haute disponibilité pour l'ADDS**

Gestion de la réplication ADDS et sa sécurité  
Mise en œuvre de la sauvegarde, restauration et récupération après sinistre pour l'ADDS  
Gestion des risques de l'interruption de service  
Mise en œuvre des clusters de basculement  
Gestion des risques et plan d'action dans un environnement ADDS.

### **Atelier : Sécurisation des réplicas ADDS, Mise en place d'un cluster de basculement sécurisé**