

# Windows Server 2016 : Assurer la sécurité

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Systèmes et Réseaux

**Action collective :** Non

**Filière :** Systèmes et réseaux Microsoft

**Rubrique :** Windows Server 2019

**Code de formation :** MS20744

## € Tarifs

**Prix public :** 2920 €

### Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

**Le plan de développement des compétences de votre entreprise :** rapprochez-vous de votre service RH.

**Le dispositif FNE-Formation.**

**L'OPCO** (opérateurs de compétences) de votre entreprise.

**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

**CPF -MonCompteFormation**

Contactez nous pour plus d'information : [contact@aston-institut.com](mailto:contact@aston-institut.com)

## PRÉSENTATION

### Objectifs & compétences

- Être en mesure d'assurer la sécurité des systèmes Windows Server - Comprendre comment assurer la sécurité des infrastructures de développement et de production - Apprendre à configurer et mettre en oeuvre l'administration "Just In Time" - Disposer des connaissances nécessaires pour assurer la sécurité des données

### Public visé

- Ingénieurs système et réseau

### Pré-requis

- Avoir suivi les formations MS20740-Stockage et Virtualisation Windows Server 2016" ; MS20741- Les services réseaux Windows Server 2016" ; MS20742-Gestion des identités avec Windows Server 2016" ou posséder les connaissances et compétences équivalentes - Posséder une solide expérience sur les réseaux (TCP/IP, UDP, DNS...), les principes AD DS, la virtualisation Hyper-V et la sécurité Windows Server

## Lieux & Horaires

**Durée :** 35 heures

**Délai d'accès :** Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

## PROGRAMME

### Module 1 :

Détection des intrusions avec les outils sysinternals

Généralités Les outils Sysinternals

### Module 2 :

Protection des identifiants et des accès privilégiés

Droits utilisateur

Comptes d'ordinateur et comptes de service

Protection des identifiants

Stations dédiées et serveurs intermédiaires

Déploiement d'une solution de gestion des mots de passe d'administrateur local

### Module 3 :

Limitation des droits d'administration et principe du privilège minimal

Description Implémentation et déploiement

### Module 4 :

Gestion des accès privilégiés et forêts administratives

Le concept de forêt administrative

Introduction à Microsoft Identity

Manager Administration "Just In Time" et gestion des accès privilégiés avec Microsoft Identity Manager

### Module 5 :

Atténuation des risques liés aux logiciels malveillants

## Prochaines sessions

Consultez-nous pour les prochaines sessions.

Configuration et gestion de Microsoft Defender  
Stratégies de restrictions logicielles et AppLocker  
Configuration et utilisation de Device Guard  
Utilisation et déploiement de Enhanced Mitigation  
Experience Toolkit  
Module 6 : Méthodes d'analyse et d'audit avancées pour la surveillance de l'activité  
Introduction : l'audit système Stratégies d'audit avancées Audit et enregistrement des sessions PowerShell

**Module 7 :**

Analyse de l'activité avec Microsoft Advanced Threat Analytics et Operations  
Management suite Advanced Threat Analytics  
Présentation de OMS

**Module 8 :**

Sécurisation de l'infrastructure de virtualisation  
Infrastructures protégées (Guarded Fabric)  
Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

**Module 9 :**

Sécurisation de l'infrastructure de développement applicatif et de production  
Security Compliance Manager Nano Server Containers

**Module 10 :**

Protection des données par chiffrement  
Planification et implémentation du chiffrement EFS (Encrypting File System)  
Planification et implémentation de BitLocker

**Module 11 :**

Limitation des accès aux fichiers File Server Resource Manager (FSRM)  
Automatisation de la gestion et de la classification des fichiers  
Contrôle d'accès dynamique (Dynamic Access Control)

**Module 12 :**

Limitation des flux réseaux au moyen de pare-feu Le pare-feu Windows Pare-feu distribués  
Module 13 : Sécurisation du trafic réseau Menaces liées au réseau et règles de sécurisation des connexions Paramétrage avancé de DNS Analyse du trafic réseau avec Microsoft Message Analyzer Sécurisation et analyse du trafic SMB Module 14 : Mise à jour de Windows Server Présentation de WSUS Déploiement des mises à jour avec WSUS

**MODALITÉS****Modalités**

**Modalités :** en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

**Pédagogie :** essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

**Ressources techniques et pédagogiques :** Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

**Pendant la formation :** mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels.

**Méthode**

**Fin de formation :** entretien individuel.

**Satisfaction des participants :** questionnaire de satisfaction réalisé en fin de formation.

**Assiduité :** certificat de réalisation.

**Validations des acquis :** grille d'évaluation des acquis établie par le formateur en fin de formation.