# INTITULE DE LA FORMATION :

## Securing Windows Server 2016

## REF. COURS: MCS_20744

***CETTE FORMATION EST ÉLIGIBLE AU CPF*.**

## DUREE : 5 JOURS (35H)

- Formation inter-entreprise ou intra-entreprise
- Formation en présentiel ou distanciel
- Horaires : 9h-12h30 – 14h-17h30

## PRIX PUBLIC INTERENTREPRISES : 2860€ HT / PERS

## DESCRIPTION :

Ce cours de cinq jours, dirigé par un instructeur enseigne aux professionnels de l'informatique comment ils peuvent améliorer la sécurité de l'infrastructure informatique qu'ils administrent. Ce cours commence par souligner l'importance de supposer que des violations de réseau ont déjà eu lieu, puis vous apprend comment protéger les informations d'identification et les droits administratifs pour garantir que les administrateurs ne peuvent effectuer que les tâches dont ils ont besoin, quand ils en ont besoin.

Ce cours explique également comment vous pouvez atténuer les menaces de logiciels malveillants, identifier les problèmes de sécurité à l'aide de l'audit et de la fonctionnalité d'analyse avancée des menaces dans Windows Server 2016, sécuriser votre plate-forme de virtualisation et utiliser de nouvelles options de déploiement, telles que le serveur Nano et les conteneurs pour améliorer la sécurité. Le cours explique également comment vous pouvez aider à protéger l'accès aux fichiers en utilisant le cryptage et le contrôle d'accès dynamique, et comment vous pouvez améliorer la sécurité de votre réseau.

## OBJECTIFS PEDAGOGIQUE :

Après avoir terminé ce cours, les étudiants seront capables de :

- Sécuriser Serveur Windows.
- Développement d'applications sécurisé et infrastructure de charge de travail de serveur.
- Gérer les lignes de base de sécurité.
- Configurer et gérer l'administration juste assez et juste à temps (JIT).
- Gérer la sécurité des données.

- Configurer le pare-feu Windows et un pare-feu distribué défini par logiciel.
- Trafic réseau sécurisé.
- Sécuriser votre infrastructure de virtualisation.
- Gérer les logiciels malveillants et les menaces.
- Configurer l'audit avancé.
- Gérer les mises à jour logicielles.
- Gérer les menaces en utilisant Advanced Threat Analytics (ATA) et Microsoft Operations Management Suite (OMS).

## COMPETENCE VISEE :

## PUBLIC :

Ce cours est destiné aux professionnels de l'informatique qui ont besoin d'administrer des réseaux Windows Server 2016 en toute sécurité. Ces professionnels travaillent généralement avec des réseaux configurés en tant qu'environnements basés sur des domaines Windows Server, avec un accès géré à Internet et aux services cloud.

Les étudiants qui souhaitent obtenir une certification à l'examen 70-744 Securing Windows Server bénéficieront également de ce cours.

## PRE-REQUIS :

Les étudiants doivent avoir au moins deux ans d'expérience dans le domaine informatique et doivent avoir :

Cours terminés 740, 741 et 742, ou l'équivalent.

Une solide compréhension pratique des principes de base des réseaux, y compris TCP/IP, User Datagram Protocol (UDP) et Domain Name System (DNS).

Une solide compréhension pratique des principes des services de domaine Active Directory (AD DS).

Une solide compréhension pratique des principes fondamentaux de la virtualisation Microsoft Hyper-V.

Une compréhension des principes de sécurité de Windows Server.

## PROGRAMME :

Module 1 : Attaques, détection des violations et outils Sysinternals
Dans ce module, les étudiants découvriront la détection des violations, les types et vecteurs d'attaques, la cybercriminalité et comment vous pouvez analyser l'activité de votre système à l'aide de la suite d'outils Sysinternals.
Leçons :

- Comprendre les attaques

- Détecter les violations
- Examiner l'activité avec l'outil Sysinternals

Atelier :

- Détection de violation de base et stratégies de réponse aux incidents
- Identifier les types d'attaques
- Explorer les outils Sysinternals

Après avoir terminé ce cours, les étudiants seront capables de :

- Décrire la détection des violations.
- Décrire comment détecter une violation à l'aide des outils Sysinternals.

Module 2 : Protection des identifiants et des accès privilégiés

Ce module explique comment configurer les droits d'utilisateur et les options de sécurité, protéger les informations d'identification à l'aide de la protection des informations d'identification, implémenter des postes de travail à accès privilégié et gérer et déployer une solution de mot de passe d'administrateur local afin de pouvoir gérer les mots de passe des comptes d'administrateur local.

Leçons :

- Comprendre les droits des utilisateurs
- Comptes d'ordinateurs et de services
- Protection des identifiants
- Postes de travail à accès privilégié et serveurs de saut
- Solution de mot de passe administrateur local

Atelier :

- Implémentation des droits d'utilisateur, des options de sécurité et des comptes de service gérés par le groupe
- Configuration des options de sécurité
- Configuration des groupes restreints
- Délégation de privilèges
- Création et gestion des comptes de service gérés de groupe (MSA)
- Configuration de la fonction Credential Guard
- Localisation des comptes problématiques
- Configurer et déployer des LAP
- Installation et configuration des LAP
- Déploiement et test des LAP

A l'issue de ce module, les étudiants seront capables de :

- Comprendre les droits des utilisateurs.
- Décrire les comptes d'ordinateurs et de services.
- Aider à protéger les informations d'identification.
- Comprendre les postes de travail à accès privilégié et les serveurs de saut.
- Comprendre comment utiliser une solution de mot de passe administrateur local.

Module 3 : Limiter les droits d'administrateur avec Just Enough Administration
Ce module explique comment déployer et configurer Just Enough Administration (JEA).
Leçons :

- Comprendre JEA
- Vérification et déploiement de JEA

Atelier :

- Limiter les privilèges d'administrateur avec JEA
- Création d'un fichier de capacité de rôle
- Création d'un fichier de configuration de session
- Création d'un point de terminaison JEA
- Connexion et test d'un point de terminaison JEA
- Déploiement d'une configuration JEA sur un autre ordinateur

A l'issue de ce module, les étudiants seront capables de :

- Comprendre JEA.
- Vérifier et déployer JEA.

Module 4 : Gestion des accès privilégiés et forêts administratives
Ce module explique les concepts des forêts ESAE (Enhanced Security Administrative Environment), Microsoft Identity Manager (MIM) et Just In Time (JIT) Administration, ou Privileged Access Management.
Leçons :

- Forêts ESAE
- Présentation de Microsoft Identity Manager
- Présentation de l'administration JIT et PAM

Atelier :

- Limiter les privilèges d'administrateur avec PAM
- Approche en couches de la sécurité
- Configuration des relations d'approbation et des principaux fantômes
- Demande d'accès privilégié
- Gestion des rôles PAM

A l'issue de ce module, les étudiants seront capables de :

- Comprendre les forêts ESAE.
- Comprendre MIM.
- Comprendre l'administration JIT et PAM.

Module 5 : Atténuer les malwares et les menaces
Ce module explique comment configurer les fonctionnalités de Windows Defender, AppLocker et Device Guard.
Leçons :

- Configuration et gestion de Windows Defender
- Logiciel de restriction

- Configuration et utilisation de la fonction Device Guard
- Déploiement et utilisation de l'EMET

Atelier :

- Sécurisation des applications à l'aide d'AppLocker, de Windows Defender, des règles Device Guard et de l'EMET.
- Configuration de Windows Defender
- Configuration d'AppLocker
- Configuration de Device Guard
- Déployer et utiliser EMET

A l'issue de ce module, les étudiants seront capables de :

- Configurer et gérer Windows Defender.
- Restreindre le logiciel.
- Configurer et utiliser la fonction Device Guard.
- Utiliser et déployer l'EMET.

Module 6 : Analyser l'activité avec des audits avancés et des analyses de journaux
Ce module explique comment utiliser l'audit avancé et les transcriptions Windows PowerShell.
Leçons :

- Présentation de l'audit
- Audit avancé
- Audit et journalisation Windows PowerShell

Atelier :

- Configurer l'audit avancé
- Configuration de l'audit de l'accès au système de fichiers
- Audit des connexions de domaine
- Gestion de la configuration avancée des stratégies d'audit
- Journalisation et audit Windows PowerShell

A l'issue de ce module, les étudiants seront capables de :

- Comprendre l'audit.
- Comprendre l'audit avancé.
- Auditer et enregistrer Windows PowerShell.

Module 7 : Déploiement et configuration Advanced Threat Analytics et Microsoft Operations Management Suite
Ce module explique l'outil Microsoft Advanced Threat Analytics et la suite Microsoft Operations Management (OMS), et détaille comment vous pouvez les utiliser pour surveiller et analyser la sécurité d'un déploiement Windows Server
Leçons :

- Déploiement et configuration d'ATA
- Déploiement et configuration de Microsoft Operations Management Suite

Atelier :

- Déployer ATA et Microsoft Operations Management Suite
- Préparation et déploiement d'ATA
- Préparation et déploiement de Microsoft Operations Management Suite

A l'issue de ce module, les étudiants seront capables de :

- Déployer et configurer ATA.
- Déployer et configurer Microsoft Operations Management Suite.

Module 8 : Infrastructure de virtualisation sécurisée

Ce module explique comment configurer les machines virtuelles (VM) Guarded Fabric, y compris les exigences pour les machines virtuelles protégées et prises en charge par le chiffrement.

Leçons :

- Tissu protégé
- Machines virtuelles protégées et prises en charge par le chiffrement

Atelier :

- Guarded Fabric avec attestation de confiance de l'administrateur et VM protégées
- Déploiement d'une structure protégée avec une attestation de confiance de l'administrateur
- Déployer une VM blindée

A l'issue de ce module, les étudiants seront capables de :

- Comprendre les machines virtuelles Guarded Fabric.
- Comprendre les machines virtuelles protégées et prises en charge par le chiffrement.

Module 9 : Sécurisation du développement d'applications et de l'infrastructure de charge de travail du serveur

Ce module détaille le Security Compliance Manager, y compris la façon dont vous pouvez l'utiliser pour configurer, gérer et déployer des lignes de base. De plus, les étudiants apprendront à déployer et à configurer des conteneurs Nano Server, Microsoft Hyper-V et Windows Server.

Leçons :

- Utilisation de SCM
- Introduction au nano-serveur
- Comprendre les conteneurs

Atelier :

- Utiliser SCM
- Configuration d'une ligne de base de sécurité pour Windows Server 2016
- Déploiement d'une ligne de base de sécurité pour Windows Server 2016
- Déployer et configurer Nano Server
- Déploiement, gestion et sécurisation de Nano Server

- Déploiement, gestion et sécurisation du conteneur Windows

A l'issue de ce module, les étudiants seront capables de :

- Comprendre le SCM.
- Décrire Nano Server.
- Comprendre les conteneurs.

Module 10 : Planification et protection des données

Ce module explique comment configurer le chiffrement du système de fichiers de chiffrement (EFS) et le chiffrement du lecteur BitLocker pour protéger les données au repos

Leçons :

- Planification et mise en œuvre du chiffrement
- Planification et mise en œuvre de BitLocker

Atelier :

- Protéger les données à l'aide du chiffrement et de BitLocker
- Cryptage et récupération de l'accès aux fichiers cryptés
- Utiliser BitLocker pour protéger les données

A l'issue de ce module, les étudiants seront capables de :

- Planifier et mettre en œuvre le chiffrement.
- Planifier et implémenter BitLocker.

Module 11 : Optimiser et sécuriser les services de fichiers

Ce module explique comment optimiser les services de fichiers en configurant File Server Resource Manager (FSRM) et Distributed File System (DFS). Les étudiants apprendront comment protéger les données d'un appareil en utilisant le cryptage ou BitLocker. Les étudiants apprendront également à gérer l'accès aux fichiers partagés en configurant le contrôle d'accès dynamique (DAC).

Leçons :

- Gestionnaire de ressources du serveur de fichiers
- Mise en œuvre des tâches de gestion de la classification et de gestion des fichiers
- Contrôle d'accès dynamique

Atelier :

- Quotas et filtrage des dossiers
- Configuration des quotas du gestionnaire de ressources du serveur de fichiers
- Configuration des rapports de filtrage et de stockage des fichiers
- Implémentation du contrôle d'accès dynamique
- Préparation à la mise en œuvre du contrôle d'accès dynamique
- Implémentation du contrôle d'accès dynamique
- Validation et correction du contrôle d'accès dynamique

A l'issue de ce module, les étudiants seront capables de :

- Comprendre le gestionnaire de ressources du serveur de fichiers.

- Mettre en œuvre des tâches de gestion de la classification et de gestion des fichiers.
- Comprendre le contrôle d'accès dynamique

Module 12 : Sécurisation du trafic réseau avec pare-feu et chiffrement
Ce module explique les pares-feux qui sont présents sur Windows Server.
Leçons :

- Comprendre les menaces de sécurité liées au réseau
- Comprendre le pare-feu Windows avec sécurité avancée
- Configuration d'IPsec
- Pare-feu de centre de données

Atelier :

- Configurer le pare-feu Windows avec la sécurité avancée
- Créer et tester des règles de trafic entrant
- Créer et tester des règles sortantes
- Créer et tester des règles de sécurité de connexion

A l'issue de ce module, les étudiants seront capables de :

- Comprendre les menaces de sécurité liées au réseau.
- Comprendre le pare-feu Windows avec sécurité avancée.
- Configurer IPsec.
- Comprendre le pare-feu de centre de données.

Module 13 : Sécurisation du trafic réseau
Ce module explique comment sécuriser le trafic réseau et comment utiliser Microsoft Message Analyzer, le chiffrement SMB (Server Message Block) et les extensions DNSSEC (Domain Name System Security Extensions).
Leçons :

- Menaces de sécurité liées au réseau et règles de sécurité de connexion
- Configuration des paramètres DNS avancés
- Examen du trafic réseau avec Microsoft Message Analyzer
- Sécurisation du trafic SMB et analyse du trafic SMB

Atelier :

- Sécurisation du DNS
- Configurer et tester DNSSEC
- Configuration des stratégies DNS et RRL
- Microsoft Message Analyzer et chiffrement SMB
- Installation et utilisation de l'analyseur de messages
- Configuration et vérification du chiffrement SMB sur les partages SMB

A l'issue de ce module, les étudiants seront capables de :

- Configurer les paramètres DNS avancés.
- Examiner le trafic réseau avec Message Analyzer.
- Sécuriser le trafic SMB et analyser le trafic SMB.

Module 14 : Mise à jour de Windows Server
Ce module explique comment utiliser Windows Server Update Services (WSUS) pour déployer des mises à jour sur les serveurs et clients Windows.
Leçons :

- Présentation de WSUS
- Déploiement des mises à jour à l'aide de WSUS

Atelier :

- Implémentation de la gestion des mises à jour
- Implémentation du rôle de serveur WSUS
- Configuration des paramètres de mise à jour
- Approbation et déploiement d'une mise à jour à l'aide de WSUS

A l'issue de ce module, les étudiants seront capables de :

- Comprendre WSUS.
- Déployer les mises à jour avec WSUS.

## TEST AND CERTIFICATION :

## EVALUATION DE LA FORMATION :

- Avant la formation : Auto-positionnement du stagiaire selon les prérequis
- Pendant la formation (démarche formative) : évaluation continue des connaissances, travaux pratiques.
- À l'issue de la formation (démarche sommative) : questionnaire de satisfaction du stagiaire,
- A 6 mois : évaluation différée

## INTERVENANT :

- Consultant/ Formateur habilité et certifié Microsoft

## LIEU ET DELAI D'ACCES

- Lieu en présentiel : **38 rue Victor Hugo – 92400 COURBEVOIE ou autre site préciser dans la convocation**
- **Présentiel** : groupe de 4 participants minimum et 12 participants maximum
- **Distanciel** : groupe de 4 participants minimum et 10 participants maximum
- **Le délai estimé** entre la demande du bénéficiaire et le début de la prestation est estimé entre 3 mois et 1 jour (financement CPF).

## METHODES MOBILISEES EN DISTANCIEL

ARROW ECS Education adapte ses modules en distanciel avec l'outil TEAMS (autre selon contraintes techniques), autour de l'organisation et des principes pédagogiques suivants:

nécessaire et un tuto pour suivre la formation à distance avec l'outil TEAMS. Il valide avec chacun le bon fonctionnement des connections audio et vidéo lors d'un RV technique collectif. Il pose également les règles du jeu d'un fonctionnement en virtuel et gère d'éventuelles problématiques techniques.

Par ailleurs il est disponible la première demi-journée de formation en cas de soucis technique des participants, pour gérer individuellement d'éventuels ajustements liés à l'outil « en ligne ».

- Des documents sont envoyés en amont (par mail) : questionnaire, supports bénéficiaires, auto-tests éventuels, boite à outils …
- La « classe virtuelle » permet aux participants d'avoir accès aux mêmes ressources techniques qu'en présentiel. Chaque participant aura accès à un support de cours et un environnement technique accessible via le Cloud. Cette démarche vise à renforcer la dimension opérationnelle des sessions à distance, tout en gardant la richesse du partage en intelligence collective.

  Au-delà de l'animation en plénière, l'outil en ligne permet l'organisation de sous-groupes virtuels de travail dans le déroulé de la formation et le formateur passe d'un groupe à l'autre en soutien. De même les mises en situation sont maintenues.
  Une messagerie (chat) permet aux participants d'interagir par écrit, au-delà des échanges interactifs.

## MOYENS PEDAGOGIQUES ET TECHNIQUES

- Supports en Anglais : les participants recevront le support de la formation en format numérisé. Un lien d'accès à une plateforme de téléchargement dédiée leur sera adressé avant la formation, leur permettant de télécharger l'ensemble des supports, documentations et outils de la formation.
- Matériel nécessaire pour la formation en présentiel :

✓ Une salle dont la taille est compatible avec le plan gouvernemental de lutte contre l'épidémie de COVID-19 en vigueur au moment de la formation
✓ Un vidéo projecteur et la possibilité de sonorisation
✓ 1 paperboard
✓ Une connexion internet
✓ Un PC

- Matériel nécessaire pour la formation en distanciel :

✓ Un ordinateur comprenant un micro, une enceinte et si possible un double écran.
✓ Une connexion Internet.

## MODALITES DE SUIVI

- La convocation et le livret d'accueil sont envoyés à l'apprenant 10 jours avant le début de la formation.

- L'intervenant ou ARROW ECS Education remet le règlement intérieur, signe et fait signer la feuille d'émargement au stagiaire par demi-journées.
- L'attestation de formation est remise au stagiaire à la fin de la formation.
- Le livret d'accueil et le règlement intérieur sont consultables sur notre site https://edu.arrow.com/fr/ rubrique « ressources ».

- Suivi post formation : le participant envoie sa demande au formateur par écrit à l'adresse mail suivante : training.ecs.fr@arrow.com . Le formateur lui répond par retour de mail, sous 3 jours en fonction de ses disponibilités. Selon le niveau de complexité de la demande, il peut également lui proposer un rendez-vous téléphonique dans les cinq jours pour approfondir la question et solutionner sa problématique. Cette assistance est mise en place durant trois mois, à partir de la fin de la session.

## ACCESSIBILITE ET PRISE EN COMPTE DES SITUATIONS DE HANDICAP

- Pour nos formations, nous faisons une étude préalable à la formation pour adapter nos locaux, nos modalités pédagogiques et d'animation en fonction de la situation de handicap portée à notre connaissance. En fonction des besoins spécifiques, nous mettrons tout en œuvre avec nos partenaires spécialisés pour être en capacité de réaliser la prestation.
- Pour toute demande, merci de bien vouloir contacter notre référent handicap Cédric BOUTROS par mail : cedric.boutros@arrow.com

## MOYENS D'ENCADREMENT

- **Assistance pédagogique** : Thierry DESOUCHE – thierry.desouche@arrow.com – 06 85 34 81 53 - du lundi au vendredi (9h30-13h, 14h-17h30)
- **Assistance technique :** Jean Yves BORG – jean-yves.borg@arrow.com - – 06 76 98 76 61 - du lundi. au vend.(9h30-13h,14h-17h30)
- **Intervenant** : (préciser son nom) training.ecs.fr@arrow.com – 01 49 97 49 51 du lundi au vendredi (9h30-13h, 14h-17h30)
- **Référent handicap** : Cédric. BOUTROS – cedric.boutros@arrow.com – 06 38 14 03 69 (9h30-13h, 14h-17h30)

## DEBOUCHES ET SUITE DU PARCOURS

En France et dans l'OCDE les mutations économiques, technologiques mais aussi sociétales s'accélèrent depuis ces dernières années et incitent les entreprises à modifier en profondeur leur organisation du travail, pour anticiper les changements et de s'y adapter. Dans ce contexte, le développement et l'adaptation des compétences à ces évolutions prend une dimension primordiale, pour permettre aux équipes d'être en adéquation avec la mutation technologique en perpétuelle évolution et des nouvelles compétences techniques nécessaires.

L'accompagnement des équipes dans un environnement apprenant est devenu aujourd'hui un enjeu majeur pour permettre aux structures de déployer et réussir la transformation, mais aussi pour donner la capacité aux individus à maintenir leur employabilité ou à intégrer le marché du travail.

Cette formation vous permet de développer vos compétences et d'être en capacité de gérer la Sécurisation de Windows Server 2016.