# WINDOWS SERVER 2016 ASSURER LA SÉCURITÉ DE L'INFRASTRUCTURE MICROSOFT

| | |
|---|---|
| **Public** | Ingénieurs système et réseau opérant dans des environnements Windows complexes, comportant notamment des accès Cloud et Internet |
| **Durée** | 5 jours - 35 heures |
| **Pré-requis** | Posséder une solide expérience sur les réseaux (TCP/IP, UDP, DNS...), les principes AD DS, la virtualisation Hyper-V et la sécurité Windows Server |
| **Objectifs** | Être en mesure d'assurer la sécurité des systèmes Windows Server<br>Comprendre comment assurer la sécurité des infrastructures de développement et de production<br>Apprendre à configurer et mettre en oeuvre l'administration "Just In Time"<br>Disposer des connaissances nécessaires pour assurer la sécurité des données<br>Savoir configurer le pare-feu Windows et les pare-feux distribués<br>Être capable de sécuriser le trafic réseau et de parer les attaques<br>Apprendre à sécuriser l'infrastructure de virtualisation<br>Prendre en compte les menaces liées aux logiciels malfaisants |
| **Méthodes pédagogiques** | Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.<br>La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.<br>Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation. |
| **Moyens techniques** | 1 poste de travail complet par personne<br>De nombreux exercices d'application<br>Mise en place d'ateliers pratiques<br>Remise d'un support de cours<br>Passage de certification(s) dans le cadre du CPF<br>Remise d'une attestation de stage |
| **Modalité d'évaluation des acquis** | Evaluation des besoins et objectifs en pré et post formation<br>Evaluation technique des connaissances en pré et post formation<br>Evaluation générale du stage |
| **Planning** | Du 16/06/2025 au 20/06/2025<br>Du 15/09/2025 au 19/09/2025<br>Du 17/11/2025 au 21/11/2025 |
| **Délai d'accès** | L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session |
| **Accessibilité handicapés** | Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil. |

## DÉTECTION DES INTRUSIONS AVEC LES OUTILS SYSINTERNALS

- Généralités
- Les outils Sysinternals

## 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

## LIMITATION DES DROITS D'ADMINISTRATION ET PRINCIPE DU PRIVILÈGE MINIMAL

- Description
- Implémentation et déploiement

## 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

## ATTÉNUATION DES RISQUES LIÉS AUX LOGICIELS MALFAISANTS

- 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

## 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

## ANALYSE DE L'ACTIVITÉ AVEC MICROSOFT ADVANCED THREAT ANALYTICS ET OPERATIONS MANAGEMENT SUITE

- Advanced Threat Analytics
- Présentation de OMS

## SÉCURISATION DE L'INFRASTRUCTURE DE VIRTUALISATION

- Infrastructures protégées (Guarded Fabric)
- Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

## SÉCURISATION DE L'INFRASTRUCTURE DE DÉVELOPPEMENT APPLICATIF ET DE PRODUCTION

- Security Compliance Manager
- Nano Server
- Containers

## PROTECTION DES DONNÉES PAR CHIFFREMENT

- Planification et implémentation du chiffrement EFS (Encrypting File System)
- Planification et implémentation de BitLocker

## 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)

## LIMITATION DES FLUX RÉSEAUX AU MOYEN DE PARE-FEU

- Le pare-feu Windows
- Pare-feu distribués

## 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

## MISE À JOUR DE WINDOWS SERVER

- Présentation de WSUS
- Déploiement des mises à jour avec WSUS

## NOUS CONTACTER

**Siège social**
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

**Centre de formation**
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

**Téléphone**
04 76 23 20 50 - 06 81 73 19 35

**E-mail**
contact@audit-conseil-formation.com

**Suivez-nous sur les réseaux sociaux, rejoignez la communauté !**

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation