Windows Server 2019/2022 – Mise en œuvre de la sécurité

Programme *(Mis à jour le 12/02/2021)*

Détection des intrusions avec les outils sysinternals

- Généralités
- Les outils Sysinternals

Protections 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

Gestions 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 opérations 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

Référence

THIS2133

Durée

5 jours / 35 heures

Prix HT / stagiaire

2750€

Objectifs pédagogiques

- Assurer la sécurité des systèmes Windows Server, des infrastructures de développement et de production
- Concevoir et configurer l'administration « Just In Time »
- Gérer la configuration du pare-feu Windows et des pare-feu distribués pour sécuriser le trafic réseau et de parer les attaques
- Sécuriser l'infrastructure de virtualisation

Niveau requis

- Avoir suivi les formations « Windows Server – Stockage et virtualisation », « Windows Server – Les services réseaux » et « Windows Server Gestion des identités » ou posséder les connaissances 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

Public concerné

- Ingénieurs système et réseau opérant dans des environnements Windows complexes, comportant notamment des accès Cloud et Internet

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de

- 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 aux moyens 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