775 route de l'aérodrome
ZA Agroparc
84000 Avignon
Tél 04 90 85 98 12
Fax 04 90 86 26 24
info@cit.fr
www.cit.fr

Windows Server 2016 – Assurer la sécurité

Objectif : Acquérir les connaissances et compétences pour améliorer la sécurité d'une infrastructure IT. Apprendre à protéger les informations d'identification et les droits administratifs afin de s'assurer que les administrateurs ne peuvent exécuter que les tâches dont ils ont besoin lorsqu'ils en ont besoin. Comprendre comment vous pouvez atténuer les menaces de logiciels malveillants, identifier les problèmes de sécurité en utilisant l'audit et la fonctionnalité Advanced Threat Analisys dans Windows Server 2016, sécuriser votre plateforme de virtualisation et utiliser de nouvelles options de déploiement, comme les Nano servers et les conteneurs. Comprendre également comment vous pouvez contribuer à protéger l'accès aux fichiers en utilisant le cryptage et le contrôle d'accès dynamique et comment améliorer la sécurité de votre réseau
Prérequis : Expérience de travail avec Windows Server 2008/2012 ; connaissance des topologies et architectures réseau telles que les réseaux LAN, WAN le protocole TCP/IP, UDP, DNS, les principes AD DS et les fondamentaux de Hyper-V et de la virtualisation ;

- 5 jours -

Déroulé de l'action

- **Type de stage**

  Session Inter-entreprises
  Session Intra

- **Horaires**

  9H00-12H30 /13H30-17H00

- **Méthode pédagogique**

  Alternance exposés théoriques et exercices pratiques

- **Suivi et assistance**

  Support de cours adapté au logiciel étudié et au niveau suivi
  Assistance téléphonique gratuite et illimitée

- **Validation des acquis**

  Exercice de validation en fin d'action

Détecter les brèches et utiliser les outils Sysinternals

- Vue d'ensemble de la détection des brèches
- Utilisation des outils Sysinternals pour détecter les brèches

Protéger les "credentials" et les accès privilégiés

- Compréhension des droits utilisateurs
- Comptes d'ordinateurs et comptes de service
- Protection des "credentials"
- Compréhension des stations de travail avec accès privilégiés et les serveurs Jump
- Déploiement d'une solution locale de mot de passe administrateur (LAPs)

Restreindre les droits administrateurs avec JEA

- Comprendre JEA
- Configuration et déploiement de JEA

Gérer les accès privilégiés et les forêts administratives

- Compréhension du concept des forêts ESAE
- Introduction à MIM (Microsoft Identity Manager)
- Mise en oeuvre de JIT (Just In Time) et la gestion des accès privilégiés via MIM

Limiter les malwares et les menaces

- Configuration et gestion de Windows Defender
- Utilisation des stratégies de restrictions logicielles (SRPs) et AppLocker
- Configuration et utilisation de Device Guard
- Utilisation et déploiement du toolkit Enhanced Mitigation Experience (EMET)

Analyser les activités via l'audit avancé

- Vue d'ensemble de l'audit
- Compréhension de l'audit avancé
- Configuration de l'audit et de la connexion Windows PowerShell

775 route de l'aérodrome
ZA Agroparc
84000 Avignon
Tél 04 90 85 98 12
Fax 04 90 86 26 24
info@cit.fr
www.cit.fr

Windows Server 2016 – Assurer la sécurité

Analyser les activités avec la fonctionnalité ATA et OMS

- Vue d'ensemble de Advanced Threat Analytics (ATA)
- Compréhension d'Operations Management Suite (OMS)

Sécuriser le développement d'application et l'infrastructure serveur

- Utilisation de Security Compliance Manager
- Introduction au Nano servers
- Compréhension des conteneurs

Protéger les données avec le cryptage

- Planification et implémentation du cryptage
- Planification et implémentation de BitLocker

Limiter l'accès aux fichiers et aux dossiers

- Introduction à File Server Resource Manager (FSRM)
- Mise en œuvre de la gestion de la classification et des tâches liées à la gestion des fichiers
- Compréhension de Dynamic Access Control (DAC)

Utiliser des firewalls pour contrôler le trafic

- Compréhension de Windows Firewall
- Firewalls software-defined distribués

Sécuriser le trafic réseau

- Menaces contre la sécurité du réseau et règles de sécurité pour la connexion
- Configuration des paramètres avancés de DNS
- Analyse du trafic réseau avec Microsoft Message Analyzer
- Sécurisation et analyse du trafic SMB

Mettre à jour de Windows Server

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

Déroulé de l'action

- **Type de stage**

  Session Inter-entreprises
  Session Intra

- **Horaires**

  9H00-12H30 /13H30-17H00

- **Méthode pédagogique**

  Alternance exposés théoriques et exercices pratiques

- **Suivi et assistance**

  Support de cours adapté au logiciel étudié et au niveau suivi
  Assistance téléphonique gratuite et illimitée

- **Validation des acquis**

  Exercice de validation en fin d'action