Microsoft

Sécurité - Sécuriser Windows Server

Workshop*PLUS*

Public concerné :

Cet atelier s'adresse aux professionnels de l'informatique qui déploient, conçoivent et implémentent les environnements Windows Server:

- *Administrateurs informatiques*
- *Ingénieurs d'infrastructure Windows*
- *Administrateurs de serveurs*
- *Personnel de sécurité informatique et administrateurs*

Principales caractéristiques et avantages

Labs hébergés online

Introduction

Le Workshop Sécurité – Sécuriser Windows Server, d'une durée de quatre jours, fournit aux stagiaires les compétences nécessaires pour garantir la sécurité et la protection des serveurs contre les accès indésirables ou les intrusions. Ce cours aborde les menaces de sécurité, les contre-mesures de modélisation des menaces et les stratégies, outils et meilleures pratiques de Windows Server 2016 pour la sécurisation complète des serveurs du système de fichiers, des applications et des communications serveur sur un réseau. L'atelier se concentre également sur l'utilisation des fonctionnalités de sécurité de Windows Server 2016 pour vous aider à détecter et à vous protéger contre les menaces de sécurité qui ciblent vos ressources organisationnelles les plus précieuses.

L'atelier contient du contenu de niveau 200+ qui couvre les personnes et les processus ainsi que des sujets de sécurité technique. Ainsi, bien qu'il couvre des concepts techniques, c'est un équilibre entre le processus et la technologie qui mène à la défense en profondeur. Dans cet atelier, nous présentons les risques de sécurité communs à chaque couche de sécurité dans le modèle de défense en profondeur et discutons des atténuations de ces risques.

S'il vous plaît, veuillez consulter les informations sur l'audience cible et contacter votre représentant Microsoft Services pour vous assurer que cet atelier est adapté à votre expérience et à votre expertise technique.

Plus-values techniques

Après avoir suivi cette formation, vous serez en mesure de :

- Comprendre les menaces de sécurité les plus courantes et les contre-mesures Windows Server les plus efficaces à leur encontre.
- Protégez un serveur contre tout accès non autorisé pendant et après les processus de connexion et d'authentification.
- Protéger un environnement contre les risques liés aux logiciels inutiles et aux paramètres non sécurisés.
- Correctement sécuriser des applications en utilisant les outils et techniques Windows Server 2016 appropriés.

Prérequis

Les étudiants doivent posséder les connaissances suivantes :

- ***Les menaces et les vulnérabilités de sécurité***
- ***Gestion des correctifs***
- ***Gestion des stratégies de groupe***
- ***Pare-feu Windows***
- ***Concepts de sécurité réseau***

Matériel requis :

- ***Les étudiants devraient suivre le cours avec leurs propres ordinateurs portables afin de profiter des exercices pratiques (Labs) en Learning-on-Demand.***

Programme

Cet atelier dure 4 jours complets. Les participants sont invités à respecter les horaires. Les départs anticipés ne sont pas recommandés.

Module 01 : Menace sur la sécurité. Ce module fournit une vue d'ensemble de l'impact de la sécurité, des vulnérabilités générales, des menaces et de la protection de sécurité par Tiers, protégeant le tissu de virtualisation. Il couvre les techniques d'atténuation des attaques de type Pass-the-Hash.

Module 02 : Introduction à la modélisation des menaces. Ce module présente des sujets couvrant SDL et l'essentiel de la modélisation des menaces.

Module 03 : Renforcer les serveurs. Ce module détaille les outils qui vous aident à définir les lignes de base de sécurité, les outils recommandés par Microsoft et à appliquer les paramètres de sécurité sur un grand nombre de systèmes.

Module 04 : Atténuer le vol des informations d'identification. Ce module fournit des bases pour comprendre le vol des informations d'identification et introduit des concepts tels que les modèles de modélisation et de confinement par Tiers, ainsi que l'utilisation d'IPSec pour sécuriser le trafic et les identités.

Module 05 : Atténuer le vol des informations d'identification – approche moderne. Dans ce module, nous irons un peu plus loin, et des sujets fondamentaux tels que l'administration Just Enough et Just In Time seront couverts. Nous le compléterons avec Credential Guard.

Module 06 : Systèmes de sécurité - approche moderne. Ce module se concentre sur de nouveaux concepts dans la sécurisation des serveurs Windows, y compris Device Guard, Code Integrity Policies et Guarded Fabric.

Module 07 Architecture de sécurité. Dans l'informatique aujourd'hui, sécuriser uniquement les points de terminaison ne résoudra pas tous les défis. Construire et comprendre l'architecture jouent un rôle clé. Ces leçons couvrent les stations d'administration sécurisées et les environnements d'administration sécurisés.